Physical Security: 150 Things You Should Know

Second Edition

Lawrence J. Fennelly, CPOI, CSSI, CHL-III, CSSP-1

Marianna A. Perry, M.S., CPP, CSSP-1

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier

Butterworth-Heinemann is an imprint of Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-0-12-809487-7

Publisher: Candice Janco
Acquisition Editor: Sara Scott
Editorial Project Manager: Hilary Carr
Production Project Manager: Punithavathy Govindaradjane
Designer: Matthew Limbert
Cover Image Credit: Karen Camilovic with Camilovic Creative

Typeset by TNQ Books and Journals

The Industry has become aware of Cyber-security challenges, but few have a plan. Many will be unprepared for IT and Cyber requirements from end users. Education is the key.

Fredrik Nilsson, 2016

My wife, Annmarie and I wish to dedicate this book to our lovely daughter, Alison-Margaret Boyce, graduate of Holy Cross and mother of two outstanding college students, sister to three brothers and married to Charles E. Boyce, Esq.
Larry Fennelly

I dedicate this book to Larry Fennelly, a wonderful friend, writing partner and mentor. Thank you.
Marianna Perry.

In Memoriam

Louis A. Tyska, CPP, Past President of ASIS, Lou, and I wrote this as well as several other books for our profession. We were not just partners but best friends; his writing was pure and he saw things not as they were but how they should be.

Foreword

The title *Physical Security: 150 Things You Should Know* is truly a catchall title that includes a multitude of topics not common in other books? Active shooter/active assailant incidents, stabbings, and random unthinkable acts of violence are present in our workplaces and at our educational campuses weekly. We cannot escape these mindless crimes and thefts that impact every segment of the security management operation. *Security matters* more now than ever. Trying to decide which security concepts are right for your organization is a daunting full time task. However, I would suggest you start off with an assessment professionally done, so that you can identify your complex's needs.

This book is your road map to decoding and developing an effective security strategy beginning with the design build phase and addressing everything in between including life safety issues. Larry Fennelly and Marianna Perry have the knowledge and experience to see these complicated and ever-changing security challenges from a unique and multifaceted viewpoint. They both share their insight with the reader, and therefore every security practitioner needs to read this book. Most security books focus on one topic, i.e., risk analysis or security surveillance systems (CCTV) and access control. I love this text because it has so much material in it that we need to address our everyday problems.

Today's security books are more and more complicated and technical. We as practitioners must stay ahead of the curve, to keep up. Thomas Norman, CPP; David Paterson, CPP; Sandi Davis (Woman in Security); James Broder, CPP; Michael Fagel PhD; and Dr. Jennifer Hestermann, these practioners are our future educators along with Larry Fennelly and Marianna Perry. Writing a book title 150 Things…. etc. was not an easy task. I commend these authors and those who I mentioned for their vision and dedication will keep us ahead of the curve.

Linda Watson, MA, CPP, CSC, CHS-V
Whirlaway Group LLC

PART

Property Management 1

1. WHAT IS PHYSICAL SECURITY?

There are different opinions and interpretations about exactly what physical security is, but the two definitions below incorporate all the aspects and are all-inclusive.

The American Society for Industrial Security (ASIS) International (2005) defines *physical security* as follows:

> *Physical security focuses on the protection of people, property, and facilities through the use of security forces, security systems, and security procedures. Physical security personnel oversee proprietary or contract uniformed security operations, identify security system requirements, assess internal and external threats to assets, and develop policies, plans, procedures, and physical safeguards to counter those threats. Physical security can include the use of barriers, alarms, locks, access control systems, protective lighting, CCTV, and other state-of-the-art security technology.*[1]

The Army Field Manual, No. 3–19.30 defines *physical security* as "that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard against espionage, sabotage, damage, and theft."[2]

2. EFFECTIVE PHYSICAL SECURITY

Someone has to question design, development, and event planning decisions. Do you think that anyone from the police department or fire department for that matter asked the builder of a major hotel in Kansas City whether they had extra steel reinforcing rods left over when they built the cross-bridge that fell and resulted in many deaths and injuries? Did anyone ask the planners how the downtown pedestrian malls would respond when the "Flash Mob" fad swept the country in early 2000–16? No! *Major planning mistakes were made then and continue to be made because no one is asking the right questions*.

- *People*: Will always be the number one aspect in security. Their motivation and training make it work.
- *Policy/procedure*: Allows for easy enforcement.

[1] www.asisonline.org.

[2] *Army Field Manual, No. 3–19.30.* Headquarters Department of the Army, Washington, DC; 8 January, 2001. p. 9.

Physical Security: 150 Things You Should Know. http://dx.doi.org/10.1016/B978-0-12-809487-7.00001-2

- *Hardware*: Must be state of the art and highly reliable.
- *Facilities*: Although each complex may look different in shape and design, the principles and concepts are the same.
- *Information*: Proactive responses and documentation are needed.
- *Human resources department*: A critical area, especially when the termination of an employee is to take place. For example, access cards will need to be disabled and ID badges need to be returned/recovered along with any keys to mechanical locks.

3. SITE AND TARGET HARDENING

Some factors to consider when hardening a site or facility include:

1. Layered security or defense in depth—a single protection approach is not effective, but instead a series of levels that complement each other are needed.[3]
   a. The ASIS security glossary (2006) defines layered security as, "a physical security approach that requires a criminal to penetrate or overcome a series of security layers before reaching the target. The layers might be perimeter barriers, building or area protection with locks, CCTV and guards' and point and trap protection using safes, vaults, and sensors."[4]
2. Standoff distance—the distance between a critical asset and the nearest point of attack.
   a. The Department of Homeland Security has designed a standard standoff distance chart to protect critical assets, such as buildings and areas, from the effects of a bomb blast.[5]
3. Structural integrity of the premises—against attacks and natural disasters.
   a. Structural integrity can be assessed to determine how reliable a structure is to be able to withstand day-to-day activities as well as natural and man-made disasters.
4. Redundancy of operation systems—such as power; heating, ventilation, and air conditioning (HVAC); and communications systems.
   a. Have backup systems that are in place and tested to endure operability.

   Sample recommendations are as follows:

- The HVAC exterior intakes should be protected to prevent the introduction of harmful materials into the intake systems. Some buildings place air intakes high above the ground or on the roof, whereas others use physical barriers to prevent unauthorized access to the air intakes. Intrusion detection devices, video surveillance, and/or security officers may be utilized.

[3] *Physical security principles.* ASIS International Publishers, VA, 2015.
[4] Ibid; http://www.hitechcj.com/homelandsecurity/bomb_threat_stand_off_distances.html.
[5] http://www.hitechcj.com/homelandsecurity/bomb_threat_stand_off_distances.html.

- Air intakes exhaust and ventilation openings greater than 10 in. in diameter should be secured and/or monitored to prevent unauthorized access to or the introduction of a biological agent into the building.[6]
- It should be ensured that there is no subterranean access to buildings through underground utility openings such as water intakes, sewers, vents, or ducts. Any opening larger than 96 in. should be protected with welded bar grills. An alternative to one large pipe with access into the facility is the construction of multiple pipes, each having a diameter of less than 10 in. but with the same capacity as the one large pipe.[6]
- It should be ensured that there is no access to buildings through roof-mounted air returns, ventilation louvers, or maintenance hatches.

Additionally, we have 10 items listed below to consider as part of your physical security program:

1. Use effective lockdown procedures and products.
2. Make window glazing impact and bullet resistant.
3. Improve access control with appropriate visitor screening.
4. Identify sexual predators.
5. Stay current on real-time crime and local incident data.
6. Utilize duress alarms for additional immediate response.
7. Use mass notification tools like beacons, digital signage, public address systems, and electronic device alerts.
8. Maximize entry/exit door security.
9. Utilize internet protocol (IP) cameras with effective storage capabilities.
10. Expedite response time of emergency response personnel.

4. PHYSICAL BARRIERS

Physical barriers are typically separated into the following categories:

- Doors and windows, plus other openings
- Window film, blast curtains, and shutters
- Floors
- Roofs
- Fences and walls and gates
- Natural barriers and water obstacles, planters
- Bollards, jersey barriers, and rising wedge systems

The emphasis on design and use deviates from the target-hardening approach to crime prevention. Traditional target hardening focuses predominantly on denying access to a crime target through physical or artificial barrier techniques such as walls, fences, gates, locks, grilles, and the like. Target hardening often leads to

[6]ASIS International, Protection of Assets Manual; 2008.

constraints on use, access, and enjoyment of the hardened environment. Moreover, the traditional approach tends to overlook opportunities for natural access control and surveillance. The term natural refers to deriving access control and surveillance results as a by-product of the normal and routine use of the environment. It is possible to adapt normal and natural uses of the environment to accomplish the effects of artificial or mechanical hardening and surveillance. Nevertheless, Crime Prevention Through Environmental Design (CPTED) employs pure target-hardening strategies, either to test their effectiveness compared with natural strategies or when they appear to be justified as not unduly impairing the effective use of the environment.

DESIGN

- How well does the physical design support the intended function?
- How well does the physical design support the definition of the desired or accepted behaviors?
- Does the physical design conflict with or impede the productive use of the space or the proper functioning of the intended human activity?
- Is there confusion or conflict in terms of the manner in which the physical design is intended to control behavior?

The three CPTED strategies of territorial reinforcement, natural access control, and natural surveillance are inherent in the Three-D concept. Does the space clearly belong to someone or some group? Is the intended use clearly defined? Does the physical design match the intended use? Does the design provide the means for normal users to naturally control the activities, to control access, and to provide surveillance? Once a basic self-assessment has been conducted, the three Ds may then be turned around as a simple means of guiding decisions about what to do with human space. The proper functions have to be matched with the space that can support them—with space that can effectively support territorial identity, natural access control, and surveillance—and intended behaviors have to be indisputable and be reinforced in social, cultural, legal, and administrative terms or norms. The design has to ensure that the intended activity can function well, and it has to directly support the control of behavior.

5. BARRIER PLANNING[7]

When planning perimeter barriers, take into consideration the following:

1. Walls are usually more expensive than fences, observation enclosures, and security surveillance systems [closed-circuit television (CCTV)].
2. Fences and walls provide only limited delay against intruders, and the least secure types can only delay a skilled intruder for a few seconds. Perimeter barriers intended to provide protection against intruders should therefore be considered delay devices only.

[7] John J Fay, CPP, B-H. *Model security, policies, plans and procedures*. Elsevier; 1999.

Therefore, the combination of a fence or wall with security lighting, an intruder detection system, a CCTV, and a security officer.
3. The perimeter should be as short as possible and illuminated.
4. The perimeter should run in straight lines between comer posts to facilitate surveillance.
5. Drains or culverts giving access beneath the perimeter barrier should be protected.
6. The ground on both sides of the perimeter barrier should be cleared to deny cover to an intruder.
7. Emergency gates may be required to prove safe evacuation routes.
8. A sterile zone protected by a double fence may be required for certain types of intruder detection sensors.

6. ASIS INTERNATIONAL STANDARDS AND GUIDELINES[8]

ASIS International is the worldwide leader in security standards development and is an American National Standards Institute (ANSI)–accredited standards developer.

SECURITY MANAGEMENT STANDARD: PHYSICAL ASSET PROTECTION

This Standard presents a comprehensive management approach for the protection of assets by the application of security measures for physical asset protection. It provides generic principles, requirements, and guidance as well as the framework for a management system to assist organizations in the design, implementation, monitoring, evaluation, maintenance, and replacement of physical protection systems. All the requirements and guidance in this Standard are intended to be incorporated in the ANSI/ASIS SPC.1-2009 Organizational Resilience Standard, or any type of an organization's management system based on the PDCA model. The Standard is applicable to organizations of all sizes across all sectors: private, public, and not-for-profit sectors.

The ASIS International offers guidelines that are a collection of suggested practices aimed at increasing information awareness.

FACILITIES PHYSICAL SECURITY MEASURES GUIDELINE

This Guideline assists in the identification of physical security measures that can be applied at facilities to safeguard or protect an organization's assets-people, property, and information. This Guideline outlines eight main categories of physical security measures used to protect facilities: CPTED, physical barriers and site hardening, physical entry and access controls, security lighting, intrusion detection systems,

[8] https://www.asisonline.org/Standards-Guidelines/Guidelines/Pages/default.aspx.

video surveillance, security personnel, and security policies and procedures. It also provides an updated list, which is as follows:

INVESTIGATIONS

Provides guidance on establishing investigative programs as well as the conduct of individual investigations, including the competence and evaluation of investigations.

RISK ASSESSMENT

Provides guidance on developing and sustaining a coherent and effective risk assessment program including principles, managing an overall risk assessment program, and performing individual risk assessments, along with confirming the competencies of risk assessors and understanding biases.

SUPPLY CHAIN RISK MANAGEMENT: A COMPILATION OF BEST PRACTICES

Developed in collaboration with the Supply Chain Risk Leadership Council, this Standard provides a framework for collecting, developing, understanding, and implementing the current best practices for supply chain risk management.

AUDITING MANAGEMENT SYSTEMS: RISK, RESILIENCE, SECURITY, AND CONTINUITY—GUIDANCE FOR APPLICATION (SPC.2)

The SPC.2 Standard provides guidance for establishing and managing an audit program, as well as conducting individual audits consistent with the ISO 19,011 and ISO/IEC 17021 standards.

CHIEF SECURITY OFFICER—AN ORGANIZATIONAL MODEL ANSI STANDARD

The ASIS released a revised ANSI/ASIS Chief Security Officer—An Organizational Model Standard that provides a model for organizations to use when developing a senior leadership function responsible for providing comprehensive, integrated risk strategies to protect an organization from security threats. This standard replaces the 2008 ANSI/ASIS Chief Security Officer Organizational ANSI standard.

7. THE IMPORTANCE OF PHYSICAL SECURITY POLICIES AND PROCEDURES[9]

Organizations should develop security procedures for every aspect of the security operation. These procedures should protect people, property, and information, and each procedure should be connected to a security policy of the organization.

[9] Fennelly LJ. *Handbook of loss prevention and crime prevention*, 5th ed. Elsevier, Boston, MA; 2012.

Policies: Security policies are general statements of the way an organization performs business functions. Security policies establish strategic objectives and priorities for the organization. Security policies are generally issued at the executive level and emphasize the commitment of management to ensure workplace security and show due diligence to address security vulnerabilities to help keep the workplace safe.

Procedures: Security procedures are implementation instructions for personnel to comply with security policies. Procedures change more often than policies to meet the changing needs of the organization; a policy may remain in place for a long period of time, but the procedures implemented to carry out the policy may change without management involvement.

8. PHYSICAL SECURITY: 10 THINGS YOU SHOULD KNOW

1. There are different types of metal fences, but the four main types of inexpensive, metal fences are chain link, barbed tape, barbed wire, and concertina.
2. A chain-link fence should be 9-gauge wire or heavier and 6–8 ft in height, depending on the security application. The openings in the mesh should be no larger than 2 in.
3. The two kinds of protective barriers are structural and natural.
4. Barriers are psychological deterrents geared to deter, delay, and supplement security personnel.
5. Fences and/or barriers control pedestrian traffic and vehicular traffic.
6. Categories of burglary-resistant glass are plexiglas, plastic glazing, and safety glass (UL listed).
7. There are six types of basic protection available for windows: two-track storm windows, double locks on windows, double locks on sliding glass windows and doors (charley bar and secondary lock), steel bars, mesh wire, and burglary-resistant glass.
8. The weakest point in the window is the glass. Beware that the glazing compound (putty) may be removed on Monday and the glass may be removed and/or broken on Tuesday.
9. Doors come in different shapes and sizes ranging from solid core and metal to hollow core. Some have hinges on the inside, whereas some may have hinges on the outside. Some hinges may have nonremovable hinge pins.
10. The most common types of door locks are double-cylinder/double-keyed deadbolt and single cylinder/single-keyed deadbolt. Door viewers (peep holes) with a 360-degree field of view also enhance security because whoever is outside of the door can be identified before the door is opened or unlocked.

9. FENCE ENHANCEMENTS

The most commonly used barrier (other than the walls of a building) is a fence. Fences can vary in type, size, use, and effectiveness, and fences can be erected fairly

quickly at reasonable costs—depending on the specific type. It is important to balance the costs of the fence with the risk, so be sure that the specific fence type that you select meets the specific needs of the organization. Fences can be made more effective when barbed wire or concertina wire, alarm sensors, and video surveillance are added. Double fences may also be utilized with a clear zone between the fences and a clear zone on the outside of each fence.[10]

10. ASSET PROTECTION

Assets are something valuable that an entity owns, benefits from, or has use of in generating income.[11]

Asset identification is an evaluation of what to protect by considering the value of the asset to the organization. There are three steps for identifying assets: (1) specify undesirable consequences, (2) select asset identification technique, and (3) identify areas, components, or material to be protected.[12]

Asset protection brings together the functions of the organization into a comprehensive and proactive management system. It is important that the asset protection program be tied to the mission of the organization and that it "fits" with the culture of the organization. The goal of any asset protection program is to protect tangible and intangible assets by removing or reducing vulnerabilities.

11. INTERNAL THEFT

Without a doubt, internal theft is one of the most difficult issues that an organization has to deal with and is a serious threat. Any property that is left unattended and/or unsecured is at risk. Covert security surveillance systems can be a very effective tool for internal theft. Setting up of such equipment, leaving it in a specific location for weeks at a time, and catching the dishonest employee is certainly worth the investment. The report reads, "I returned from my vacation only to find XYZ gone. I'm so upset." It may be food, cash, money, equipment, and even candy (and it is not the janitors). We have used employee awareness and education programs to combat internal theft. At one location, we were having money stolen on the 12th and 26th of every month. We brought all employees into a large conference room and explained the issue and told them about every instance where money was stolen. We took out a pair of handcuffs and announced to the group, "If any more money is stolen, the thief will be wearing these bracelets as they are taken off to jail." *Our point is…be creative and come up with an approach that works. We have found that dissatisfied/disengaged employees are most frequently involved in theft.*

[10] Fennelly LJ. *Effective physical security*. Elsevier, Boston, MA; 2013.
[11] www.businessdictionary.com/definition/asset.html.
[12] Fennelly LJ. *Handbook of loss prevention and crime prevention,* 5th ed. Elsevier, Boston, MA; 2012.

Major causes of employee theft:

- Opportunity and desire
- Sense of entitlement
- Ineffective hiring and background screening processes
- No management controls (honesty, integrity, and leadership)
- No personnel controls (vacations, job duties, and training)
- No process controls (checks and balances) in place
- Personal gain
- Job dissatisfaction
- Disengaged workers
- No employee security (theft) awareness programs

12. ENVIRONMENT

The conceptual thrust of a CPTED program is that the physical environment can be manipulated to produce behavioral effects that will reduce the incidence and fear of crime, thereby improving the quality of life. These behavioral effects can be accomplished by reducing the propensity of the physical environment to support criminal behavior. Environmental design, as used in a CPTED program, is rooted in the design of the human–environment relationship. It embodies several concepts. The term *environment* includes the people and their physical and social surroundings. However, as a matter of practical necessity, the environment defined for demonstration purposes is that which has recognizable territorial and system limits. The term *design* includes physical, social, management, and law enforcement directives that seek to affect positively human behavior as people interact with their environment. Thus, the CPTED program seeks to prevent certain specified crimes (and the fear attendant on them) within a specifically defined environment by manipulating variables that are closely related to the environment itself.

The program does not purport to develop crime prevention solutions in a broad universe of human behavior but rather solutions limited to variables that can be manipulated and evaluated in the specified human–environment relationship. The CPTED involves design of physical space in the context of the needs of legitimate users of the space (physical, social, and psychological needs), the normal and expected (or intended) use of the space (the presence or absence of activity planned for the space), and the predictable behavior of both legitimate users and offenders. Therefore, in the CPTED approach, a design is proper if it recognizes the designated use of the space, defines the crime problem incidental to and the solution compatible with the designated use, and incorporates the crime prevention strategies that enhance (or at least do not impair) the effective use of the space. The CPTED draws not only on physical and urban design but also on contemporary thinking in behavioral and social science, law enforcement, and community organization.

Reducing crime through environmental security includes:

- *Increased perpetration time*: more difficult to commit the crime.
- *Increased detection time*: enhanced lighting, landscaping, etc.
- *Decreased reporting time*: better observation by more people.
- *Decreased police response time*: better planning of streets, clearly marked exits, and pathways.

13. CARD ACCESS CONTROL SYSTEMS

Card access control systems need to be multifunctional.

- Utilize "smart" cards and integrate them with other systems (e.g., parking garages or lots, time and attendance, computer systems), if possible.
- Badge to access restricted or sensitive areas can be controlled to allow access only on specific days and during designated times.
- Through the use of access card database storage determine the legal and/or organizational needs based on your specific industry.
- Have procedures in place to change access levels when an employee is transferred from one position to another within the organization.
- Have procedures in place to remove access for employees who are no longer with the organization, and audit for 100% compliance.
- Expand card access control systems to provide control at multiple sites for one organization.
- Incorporate sufficient expansion capabilities into card access control systems to allow for future growth of the organization.

14. BADGES

There are many different types of badges. Badges with color coding can be used for years of service, clearance levels, departments, and/or locations. In addition, there is video badging, which displays a corporate logo or a special design, which also may be color coded or display the employee's photograph.

When badges are initially introduced to an organization's security processes, it would appear to be a simple process, until some of the questions and concerns we have identified below arise:

1. If an employee loses the badge, it costs $10.00 to replace. Some employers allow one "free" replacement easily.
2. When an employee is fired, who retrieves the badge, keys, or other company property? Who disables the badge in the system if it is not returned?
3. If a badge is reported stolen, what is the process to render it useless (disable the badge in the system)?

4. If a badge is borrowed or used by an unauthorized person(s), have sufficient data such as height, weight, and color of eyes and hair included, using both sides of the card?
5. Who will maintain the database for badges?
6. Identification of access levels and authorization.

USE OF BAR CODES

1. Use an assigned employee number or social security number to identify the badge holder.
2. Is a tamper-proof seal used?
3. Have you considered badges for retired employees?

Whatever system you purchase, be sure that it can provide you with state-of-the-art equipment and that it has sufficient or adequate support capability.

Strive to remain current. Ask vendors and technicians questions and to explain everything you need to know about the system. Why was the system down? Call upon peers and associates and ask questions and seek advice and solutions to your problems. We learn by being inquisitive.

15. ACCESS CONTROL BASICS FOR THE SECURITY/PROTECTION OFFICER[13]

This section discusses the basics of electronic access control (EAC) systems and how they enhance the role of the protection officer.

OVERVIEW

Access control is a security method that controls the flow of traffic through the access points and areas of a protected facility. Access control is one of the primary functions of protection officers. The key element of access control is identification. This can be accomplished by having officers posted at access points and areas, using CCTV systems and electrical/mechanical controls, or by using computer-based EAC systems.

WHAT IS ELECTRONIC ACCESS CONTROL?

EAC is a method of access control that uses computer-based technology to control and monitor access. Most EAC systems use credit-card-sized access control cards that are programmed to activate devices called *card readers*. These card readers are installed at controlled locations, usually doors. In a typical system, this could be a door, turnstile, gate, or some other access point or area. The card reader's sensor extracts information from the card, translates that information into a code number,

[13] Henry CR, CPP, CPO, CFE. *IFPO protection news*. Sumner; 1998.

and sends this information to the system's computer. This number is compared with the user's programmed access information, and access is either granted or denied. Depending on the system, when access is denied an alarm may be activated. In most cases, there may be a printed record of each access transaction. This provides the system's basic audit trail.

The basic EAC system is made up of the following components:

ACCESS CARDS

1. Proximity Cards
   Proximity access cards are the most widely used cards for EAC systems. They work via the use of passively tuned circuits that have been embedded in a high-grade fiberglass epoxy card. To gain access, the card holder holds the card within 2 to 4 in. from a card reader. The reader's sensor detects the pattern of the frequencies programmed in the card. This pattern is then transmitted to the system's computer. If the pattern matches the reader's, the reader unlocks the door and records the transaction. If the pattern does not match, no access is granted and this transaction is recorded.
2. Magnetic Cards
   Magnetic cards use various kinds of materials and media to magnetically encode digital data onto cards. To gain access the card user inserts or "swipes" (passes the badge through) the card reader. As the card is withdrawn from the reader, it moves across a magnetic head, similar to that in a tape recorder head, which reads the data programmed in the card. The information read from the card is sent to the system's computer for verification. If verification is made, the computer sends a signal to the card reader to grant or deny access, and if access is granted, a signal is sent to unlock the door.

   Magnetic cards look like regular credit cards. The most popular medium for this type of access card is magnetic stripe. With this type of card, a pattern of digital data is encoded on the card's magnetic stripe. This type of card is relatively inexpensive, and a large amount of data can be stored compared with other kinds of magnetic media. These cards tend to chip and break, however, through excessive use.

   Another type of magnetic card medium uses very small dots of magnetic material that are laminated between plastic layers of the card. This type of card is cheaper to use than magnetic stripe, but its coded data can be deciphered and is subject to vandalism and wear and tear.
3. Weigand Cards
   Weigand-based access control cards use a coded pattern on magnetized wire that is embedded within the card. When this card is inserted into a reader, the reader's internal sensors are activated by the coded wire. This type of card is moderately priced and will handle large amount of traffic. It is less vulnerable to vandalism and weather effects than other types of cards. Its main deficiency is that it is subject to wear and tear.

OTHER TYPES OF ACCESS CARDS

Smart cards contain an integrated chip embedded in them. They have coded memories and microprocessors in them, hence, they are like computers. The technology in these cards offers many possibilities, particularly with proximity card–based card access control systems.

Optical cards have a pattern of light spots that can be read by a specific light source, usually infrared.

Capacitance cards used coded capacitor-sensitive material that is enclosed in the card. A current is induced when the card activates a reader. This current checks the capacitance of the card to determine the proper access code.

Some access devices come in the shape of keys, disks, or other convenient formats that provide users with access tools that look attractive and subdued, but at the same time are functional.

CARD READERS

Card readers are devices used for reading access cards. Readers come in various shapes, sizes, and configurations. The most common reader is the type in which the card user inserts the card in a slot or runs or "swipes" the card through a slot. The other type of reader uses proximity technology where the card user presents or places the card on or near the reader.

Some insertion-type card readers use keypads, where after the user inserts the card, the user enters a unique code number on the keypad. This action then grants access.

BIOMETRIC ACCESS CONTROL

As we enter the 21st century, biometric technology or the use of human biological characteristics for identification and verification, is being increasingly used in access control systems. The most popular systems use hand geometry, fingerprints, palm prints, eye retinal patterns, voice prints, and signature recognition. When biometric devices are used, they are designed and installed concurrently with card reader systems. Soon, more than one form of identification will be used.

16. TURNSTILES AND "TAILGATING"[14]

Tailgating may be a problem for your security gates. Turnstiles will decrease the everyday piggybacking by forcing people to go through a turnstile one authorized person at a time.

Optical turnstiles form pedestrian passageways to controlled areas and are typically used in upscale lobby entrances where high security, high-speed throughput, and interior esthetics are priorities. These single or bidirectional, state-of-the-art pedestrian control devices are used by the access control system to grant or deny access into a facility.

[14] Permission obtained to reproduce from Designed Security Inc. Bastrap Texas 78602.

Optical turnstiles can grant access to 30 people per minute, per lane and are versatile during peak traffic hours. Sleek bollard designs can be surfaced to match the interior of any lobby with standard or custom designs and finishes.

Compatible with all conventional access control devices, they communicate to users via visual/audible annunciation. Detection, scanning, and control electronics, located within the bollards, ensure that only one individual per valid card presented is granted access, thus preventing "tailgating."

Any attempt to enter without presenting an authorized card generates an alarm condition, which sounds a local alarm, flashes red graphics on the bollard, and trips an alarm relay output that can trigger any number of responses to prevent further access such as alerting security personnel, switching security surveillance system [closed-circuit television (CCTV)] cameras. and locking down interior doors and elevators.

ACCESS OBJECTIVES

Optical turnstiles achieve many objectives when they are properly applied. For example, they can provide the following:

- Lanes that control both access and egress—the capability of providing bidirectional travel on small applications using only one lane
- Easy integration with all card reader styles, biometric technologies, asset tracking technologies, and subsystems such as security video, duress, and intrusion detection (alarm) system (IDS)
- The ability to ensure that each person is identified by a card, biometric device, or PIN when he or she comes through the lanes
- A formidable barrier if access must be halted.

The important thing to remember about the optical turnstile is the ability to utilize the technology in a variety of applications. For example, optical turnstiles can be purchased that are simply open lanes that allow people to pass through without the use of barriers, can be supplied with "wing-style" retractable barriers similar to the one used in transportation centers such as train stations, and have arms that prevent from traveling if their path is obstructed. In addition, there is a "crash through" feature allowing barrier-free egress in the event that emergency evacuation is required.

Optical turnstiles are available with retractable glass barriers that can be installed as low glass (37 in. high), medium glass (42 in.), or high glass (67 in.), each of which open and close with every transaction. The glass height is measured from about 3 in. above floor level, and the cabinet itself is about 42 in high and mounts to the floor. Only the lane employing a high-glass retractable barrier should be installed in applications where a security officer is not in the immediate area. If the optical turnstile is in a remote location, the use of subsystem technologies, such as security video to access transaction monitoring/recording and above-the-glass IDS devices, should be

incorporated in case someone attempts to scale the glass barrier to gain entry into the facility. These technologies would be monitored at a centralized console with the ability to assess and deploy response personnel should something of this nature occur at a controlled access, optical turnstile portal.

Source: Security Magazine, August 1, 2005.

17. OPTICAL TURNSTILE SOLUTIONS AND 13 THINGS YOU SHOULD KNOW ABOUT OPTICAL TURNSTILES[15]

Optical turnstiles form pedestrian passageways to controlled areas and are typically used in upscale lobby entrances where high security, high-speed throughput, and interior esthetics are priorities. These single or bidirectional, state-of-the-art pedestrian control devices are used by the access control system to grant or deny access into a facility.

Optical turnstiles can grant access to 30 people per minute per lane and are versatile during peak traffic hours. Sleek bollard designs can be surfaced to match the interior of any lobby with standard or custom designs and finishes. Compatible with all conventional access control devices, they communicate to users via visual/audible annunciation. Detection, scanning, and control electronics, located within the bollards, ensure that only one individual per valid card presented is granted access, thus preventing "tailgating." Any attempt to enter without presenting an authorized card generates an alarm condition that sounds a local alarm, flashes red graphics on the bollard, and trips an alarm relay output that can trigger any number of responses to prevent further access such as alerting security personnel, switching security surveillance system (CCTV) cameras, and locking down interior doors and elevators.

THIRTEEN THINGS YOU SHOULD KNOW ABOUT OPTICAL TURNSTILE SOLUTIONS

1. Compatible with all reader technology.
2. Compatible with all access control systems.
3. High-speed ingress/egress—up to 30 people per minute, per lane.
4. Communicates via visual and audible annunciation.
5. Prevents tailgating.
6. Resolves issues regarding employee security, safety, theft, and accountability.
7. Can track employee time, attendance, and location.
8. Single and bidirectional options available.
9. Component packages available.
10. Standard or custom designs and finishes available.
11. Designs and price ranges to suit application and budget.

[15] Fennelly LJ. *Effective physical security,* 5th ed. Elsevier, Cambridge, MA; 2017.

12. Optical turnstiles comply with National Fire Protection Association (NFPA) 101: Life Safety Code, the Americans with Disabilities Act (ADA), and standard building codes.
13. Extra-wide units are available to accommodate wheelchairs.

18. THE SECURITY/PROTECTION OFFICER AND TECHNOLOGY TOOLS: ELECTRONIC ACCESS

An EAC system is ideally used as a part of a fully integrated facility management system. In such a system, EAC is interfaced and integrated with fire safety/life safety systems, video surveillance systems (CCTV), communications systems, and nonsecurity systems such as HVAC.

In an integrated system, EAC systems allow users to be accessed into various areas or limited areas. They can track access and provide attendance records. As a safety feature and for emergency response situations, they can determine where persons are located in facilities. In general, EAC systems are very flexible and strides in technology are making them even more so.

This section barely covers all that you need to know about EAC. The best way to learn about EAC is to actually work with EAC systems, take advantage of every opportunity to work with EAC systems, seek assignments where EAC systems are used, as well as ask questions from control room operators, your supervisors, and EAC vendors and service technicians. There are many excellent sources where you can read about EAC and related systems.

19. MAGNETOMETERS (METAL DETECTORS)

The metal detector is the most used form of security in airports. A magnetometer uses an electromagnetic field to detect metal objects, such as concealed handguns and knives, but it cannot detect ceramic or plastic weapons. Magnetometers are relatively inexpensive devices, but require more security personnel to operate them.

Simply put, a metal detector is an electromagnetic field with lines passing through a metallic object. Generation of eddy currents on a metal detector distorts the normal electromagnetic field. That is how weapons are detected.

Metal detectors are frequently used to:

- Increase security at schools.
- Increase security at transportation terminals.
- Increase security at courts, jails, and prisons.
- Protect presidents and world leaders.
- Protect spectators at sports and cultural events.

In a local school, a random inspection was implemented and the surprise inspection turned up knives, brass knuckles, mace, and two guns. Any person passing through a metal detector that trips the machines needs to be inspected further, generally with a hand-held unit. It is the operator's responsibility to make certain that every alarm be investigated.

Keep in mind that no metal detector can ever be expected to function at 100% efficiency.

Metal detectors have the following characteristics:

- They are deterrents.
- They work.
- They are durable.
- They are portable and rugged.
- They can detect weapons.
- They are adjustable.
- No touching is required.

20. DESIGNING SECURITY AND SITE LAYOUT

Designing security into a new complex should begin with interior security and then move out to the exterior of the building(s) and then to the outer perimeter of the property. Keep in mind the following points before you sit down with the architects:

- Eliminate all but essential doors and windows; the idea should be few entrances, but many exits.
- Specification of fire-resistant material throughout the interior.
- Install fire, intrusion, and environmental control systems.
- Separate shipping and receiving areas if possible.
- Ensure that the site meets ADA requirements.
- Plan for adequate lighting around the perimeter, before, during, and after construction.
- Review architectural design plans and layout.
- Plan a site assessment/site survey.
- Have interior/exterior detection systems.
- Apply natural surveillance and other CPTED principles and strategies.
- Will there be security/protection officers as well as supervision?
- Make employees aware of policy and procedures.
- Be educated of the physical security programs.
- Carry out budget planning and have 5-year plan.
- Audits/assessment/future needs.

The conclusion of your site layout report should reflect every aspect of the security operation and have measures in place to deny, deter, delay, and detect unauthorized individuals or criminal activity.

21. DESIGNING FOR SECURITY: A CHECKLIST

Some of the most important considerations that must be analyzed before designing a security protection system include the following factors:

1. Exterior perimeter protection
   a. A 6- to 8-ft chain-link fence (depending upon the application) with three strands of barbed wire at the top
   b. 8-ft walls and bushes no higher than 3 ft
   c. Video surveillance system
   d. Security/protection officers (contract or proprietary)
   e. Energy-efficient exterior lighting [type light-emitting diode (LED)]
   f. CPTED concepts and strategies
2. Entrance protection
   a. Overhead and pedestrian doors (type, strength of door frame, etc.)
   b. Windows (locks, grills, etc.)
   c. No miscellaneous entry points (roof, basement, subterranean utility access, etc.)
3. Interior protection
   a. Security policies and procedures
   b. Lighting
   c. Key or access card control
   d. Video surveillance system
   e. Special situations (hours of operation)
   f. Inventory control (computer safeguards)
   g. Safe, high-value, and security-sensitive areas
   h. Intrusion detection systems (alarm sensors)
   i. Local audible alarm versus central station alarm
4. Environmental considerations
   a. Areas of building to be protected
   b. Insurance requirements (UL listed, etc.)
   c. History of losses (loss experience)
   d. Type and demographics of employees
   e. Opening and closing procedures
   f. Fire and safety regulations and codes
   g. Delivery and shipping policies/procedures
   h. Situations peculiar to the building or industry
5. Law enforcement involvement
   a. Transmission of alarm signal
   b. Central station or direct connection to police station
   c. Municipal ordinances
   d. Police response time
   e. Neighborhood/business watch programs
   f. Formulating partnerships

22. WHAT IS CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN?

C. Ray Jefferies defined CPTED as "the proper design and effective use of the built environment can lead to a reduction in the fear and incidence of crime and improvement in the quality of life."[16]

23. CPTED STRATEGIES[17]

The definition of CPTED suggests a series of general design strategies that can be applied in any situation to improve natural access control, natural surveillance, and territorial behavior (see Photo 1).

There are three overlapping strategies in CPTED:

1. Natural access control
2. Natural surveillance
3. Territorial reinforcement

Access control and surveillance have been the primary design concepts of physical design programs. At the outset of the CPTED program, access control and surveillance systems—preexisting as conspicuous concepts in the field of CPTED—received major attention. Access control and surveillance are not mutually exclusive classifications since certain strategies achieve both and strategies in one classification typically are mutually supportive of the other. However, the operational thrust

PHOTO 1

Photo show natural surveillance, with bushes trimmed to under 3' in height.

[16] http://scholarlycommons.law.northwestern.edu.

[17] Crowe TD, Fennelly LJ. *Crime prevention through environmental design*, 3rd ed. Elsevier, Boston, MA; 2013.

of each is distinctly different, and the differences must be recognized in performing analysis, research, design, implementation, and evaluation.

Access control is a design concept directed primarily at decreasing crime opportunity. Access control strategies are typically classified as organized (e.g., security officers), mechanical (e.g., locks, lighting, and alarms), and natural (e.g., spatial definition). The primary thrust of an access control strategy is to deny access to a crime target and to create a perception of risk in offenders. Surveillance is a design concept directed primarily at keeping intruders under observation. Therefore, the primary thrust of a surveillance strategy is to facilitate observation, although it may have the effect of an access control strategy by effectively keeping intruders out because of an increased perception of risk. Surveillance strategies are typically classified as organized (e.g., police patrol), mechanical (e.g., lighting, locks, and alarms), and natural (e.g., windows).

Traditionally, access control and surveillance, as design concepts, have emphasized mechanical or organized crime prevention techniques while overlooking, minimizing, or ignoring attitudes, motivation, and use of the physical environment. More recent approaches to physical design of environments have shifted the emphasis to natural crime prevention techniques, attempting to use natural opportunities presented by the environment for crime prevention. This shift in emphasis led to the concept of territoriality (Photos 2–4). In a recent CPTED assessment we did, the area almost seemed perfect: the bushes were at right height, as were the tree branches to give natural surveillance.

The concept of territoriality (elaborated almost fully to date in the public housing environment) suggests that physical design can contribute to a sense of territoriality.

PHOTO 2

Photo shows natural surveillance.

PHOTO 3

Photo shows natural surveillance, with bushes trimmed to under 3' in height.

PHOTO 4

Photo shows natural surveillance.

PHOTO 5

Photo shows natural surveillance.

That is, physical design can create or extend a sphere of influence so that users develop a sense of proprietorship—a sense of territorial influence—and potential offenders perceive that territorial influence.

At the same time, it was recognized that natural access control and surveillance contributed to a sense of territoriality (see Photo 5), making it effective for crime prevention. Natural access control and surveillance will promote more responsiveness by users in protecting their territory (e.g., more security awareness, reporting, reacting) and promote greater perception of risk by offenders.

NATURAL SURVEILLANCE THROUGH ELECTRONICS

Video surveillance on or around your property can be a valuable tool and expand the CPTED concept of natural surveillance. Entrances to buildings, lobby areas, elevator lobbies and elevators, the perimeter of the property, and the perimeter of buildings can add effective security using surveillance, and security/protection officers can clearly identify who is entering the building or who is on the property. The pan, tilt, and zoom cameras available today can quickly respond to an area of concern and can offer a 360-degree view of the area and work in low-light conditions. For example, an emergency phone placed either in a building or in a parking lot can be observed or watched as soon as a call for assistance is made.

MAINTENANCE

Finally, care and maintenance allows for the continued use of a space for its intended purpose, as well as contributes to territorial reinforcement. Deterioration and blight

indicates less concern and control by the intended users of a site and indicates a greater tolerance of disorder. Proper maintenance protects the public health, safety, and welfare in all existing structures, residential and nonresidential, and on all existing premises by establishing minimum standards, best practices, and a master plan. Maintenance is the responsibility of the facilities manager, owners, and occupants.

Furthermore, the effort to achieve a balance between design for crime prevention and design for effective use of environments contributed to the shift in focus from organized and mechanical strategies per se to natural strategies. This was because natural strategies exploited the opportunities of the given environment both to naturally and routinely facilitate access control and surveillance, and to reinforce positive behavior in the use of the environment. The concept reflects a preference, where feasible, to reinforce existing or new activities or to otherwise reinforce the behavior of environment users so that crime prevention flows naturally and routinely from the activity being promoted.

The conceptual shift from organized and mechanical to natural strategies has oriented the CPTED program to develop plans that emphasize natural access control and surveillance and territorial reinforcement (Photo 6).

Although conceptually distinct, it is important to realize that these strategy categories tend to overlap in practice. It is perhaps most useful to think of territorial reinforcement as the umbrella concept, comprising all natural surveillance principles, which in turn comprise all access control principles. It is not practical to think of territorial reinforcement, natural surveillance, and access control as independent strategies because, for example, access control operates to denote transitional zones, not necessarily impenetrable barriers. If these symbolic or psychological barriers are to succeed in controlling access by demarcating specific spaces for specific individuals, potential offenders must perceive that unwarranted intrusion will elicit protective territorial responses from

PHOTO 6

Reflects closed-circuit television and lighting.

those who have legitimate access. Similarly, natural surveillance operates to increase the likelihood that intrusion will be observed by individuals who care but are not officially responsible for regulating the use and treatment of spaces. If people observe inappropriate behavior but do nothing about it, then the most carefully planned natural surveillance tactics are useless in terms of stopping crime and vandalism.

To implement CPTED concepts, consider the following:

- Provide a clear border definition of controlled space.
- Provide a clearly marked transition from public to semipublic to private space.
- Locate gathering areas in places with natural surveillance and access control and away from the view of potential offenders.
- Place safe activities in unsafe locations and unsafe activities in safe locations.
- Provide natural barriers to conflicting activities
- Improve the scheduling of space to provide the effective and critical intensity of uses.
- Design spaces to increase the perception of natural surveillance.
- Overcome distance and isolation through improved communications and design efficiencies, e.g., emergency telephones and pedestrian paths.
- Turn soft targets into hard targets.

24. QUESTIONS TO BE ANSWERED DURING A CPTED ASSESSMENT[18]

- Are there casual *surveillance* opportunities? If not, can they be added?
- Is there sufficient *lighting* for all vehicular and pedestrian pathways and activity areas used during hours of darkness (Photo 7)?
- Is there sufficient activity *lighting* indoors and is it supplemented by sources of natural light? Is there emergency lighting?
- Is *access* managed? If not, what combination of strategies could be used to better manage access?
- Are all *spaces designated and delineated* for specific use? If not, can they be?
- Are there *conflicts* between uses?
- Is there sufficient *capacity*? Is *crowding* creating tension, fear, or potential dangers?
- Are there expressions of pride and ownership (*territoriality*)? Can they be increased?
- Are all areas well *maintained*—kept clean and functional with no needed repairs or replacements? If not, when were they last maintained?
- Are *rules of conduct* communicated? Enforced?
- Are there *supporting activities* that enhance surveillance, access management, and social order? If not, can they be added?
- Are the grounds *legible*? Is it easy to understand where you are at any given point? Is it obvious which path or direction you need to take to arrive at a desired location?

[18] Crowe TD, Fennelly, LJ. *Crime prevention through environmental design*, 3rd ed. Elsevier, Boston, MA; 2013.

PHOTO 7

Area in need of maintenance.

- Does the *landscaping* enhance the ability to read the site? Does it provide shade and buffering where needed? Does it provide an esthetic quality? Is it accessible? Is it healthy and well maintained? Is it a problem?
- How do the site users *behave*? Is there respect for the environment? Are there areas where tensions and disorder are common?
- Is there *graffiti* or other signs of vandalism?
- Is there *CCTV or video surveillance*? If so, are they placed in prime locations? Are there other means of surveillance?
- Are there successful *CPTED applications* already in place? If so, take note and use them as positive examples.

25. CPTED ISSUES/RECOMMENDATIONS[19]

The following are some environmental problems and issues that may be documented as recommendations as part of a CPTED assessment:

- One-way street systems have been found not only to improve traffic flow but also to create dead zones for business, with resulting crime or fear of crime that deters development efforts.
- Thorough traffic in neighborhoods has been found to be detrimental to residential housing values, stability, and crime rates.

[19] Crowe TD, Fennelly, LJ. *Crime prevention through environmental design*, 3rd ed. Elsevier, Boston, MA; 2013.

- Downtown projects continue to fail by making fundamental errors that reduce natural surveillance and natural access control, resulting in the loss of desired users and domination by unwanted users.
- Fortress effects are produced by designers of convention centers, hotels, banks, senior citizen housing, and parking lot structures. These destroy the surrounding land uses and create a "no-man's land."
- Bleed-off parking enhances conflict between commercial and residential uses; both lose.
- Design and management can actually reduce business and increase victimization of employees and customers.
- Mall and major event facility parking areas with poorly planned access control and layout can produce traffic congestion and become magnets for undesirable activity.
- School and institutional designs can inadvertently create dysfunctional areas where surveillance is impossible, resulting in increased behavioral and crime problems and overall impediments to successful operations (e.g., students' achievement in schools).
- Public housing and affordable housing can become projects that serve as magnets for transients, as opposed to local poor, with further detrimental effects on existing neighborhoods.

26. MEASURING AND EVALUATING CPTED

Very little has been written on how to measure the effectiveness of a CPTED program. Let us call the site in question "the complex" since CPTED covers the full spectrum. To begin, you obtain 3 years of crime and incident data for "the complex." After a full assessment and review of the natural surveillance (landscape security), access control, and territoriality, you implement recommendations to address security vulnerabilities and "the complex" becomes a hardened target.

By definition, a deterrent is, "Serving to Deter - Relating to Deterrence."[20] Take, for example, the following situation: We were in a large building complex recently and walked past an armed security officer outside the building and a security officer inside the building in the lobby, who greeted us. "Where are you folks going today? He asked. We replied and he then called upstairs, confirmed our appointment, used his access control card for the elevator, and we were on the way to our meeting. We discovered that the elevator only went to the designated floor. After our meeting, we also found out that the elevator would only return us to the lobby on the first floor of the building—not any other floors. This is great security—deterrents and physical security working together smoothly.

The job of security/protection officers must change to be more proactive, instead of reactive. Crime data from the past must be analyzed and appropriate measures put

[20] http://www.merriam-webster.com/dictionary/deterrent.

in place. It is critical that *security/protection officers continually audit and report on the status of EVERY aspect of the physical security program—including CPTED concepts*.

AWARENESS

Become aware of your surroundings. Learn to be "situationally aware." Know who should be in your neighborhood or in your community, and most importantly, know who the strangers are. For example, you see a man walking down the street with the black dog. Do you know who he is and where he lives? Do you see behavior that is unusual or suspicious? If he looks like he does not belong, simply ask him a question. "Can I help you?" Evaluate his response to determine your next step.

Have you ever gone for a walk in your neighborhood and noticed four newspapers on the porch or on the lawn? What does that tell you? Criminals do the same assessments of potential targets to evaluate their next move.

Awareness programs such as Neighborhood or Business Watch are crime prevention and educational programs to increase community awareness so that citizens know what to look for and how to report suspicious behavior to security/protection officers or law enforcement.

FEAR OF CRIME

Neighborhood or Business Watch and other community-law enforcement partnerships are not just about crime prevention. They are about improving the overall quality of life for everyone who lives or works in the community by reducing the crime rate and also reducing the fear of crime. If an area or neighborhood is relatively safe and has a very low crime or incident rate, but the people are still afraid, your awareness and protection programs are not working. People should not be afraid. They should "feel" safe. Statistics tell us that more people have a fear of crime than are actual victims of crime.

27. VANDALISM

Vandalism is the malicious destruction of property, and it is also a crime. Vandalism can occur on both public and private properties. During the past few years, we have seen houses of worship defaced with graffiti, statues knocked over, and property destroyed. These are just a few of the items that make the news. Below is a list of acts of vandalism that many times do not make the news:

- A sign is knocked down.
- Windows are broken in a building.
- Car windows are smashed, but nothing is stolen.
- Cars are "keyed" (paint scratched).
- Trash cans are tipped over and garbage strewn about.

- Mailboxes are knocked down or broken.
- Motor vehicle tires are slashed or antennas are broken off.
- Buildings or walls are marked with graffiti or tagging.
- Graffiti is in public restrooms.

Do not allow your property to become a canvas for tagging or graffiti. Consider the use of paint or coatings that will allow for easy removal of graffiti. All graffiti or tagging should be removed within 24 h.

28. BUILDING INTERIORS[21]

Is the principal material of the exterior walls of the building one of the following materials?

1. Reinforced concrete?
2. Concrete block?
3. Brick?
4. Metal?
5. Others (specify)?

What material is used on the interior walls of the building?

1. Sheetrock?
2. Plaster?
3. Veneer on plywood?
4. Ceramic tile?
5. Other material?

Is the principal material of the building's ceilings/floors reinforced concrete or metal?

What best describes the building's interior surface ceiling material?

1. Gypsum?
2. Wood?
3. Wallboard?
4. Acoustical tile?
5. Exposed structure?
6. Other material?

Does the facility have a suspended ceiling? If so, is there a space large enough to hold a person between the suspended ceiling and the structural ceiling of the facility?

Is entry to the space between the suspended ceiling and the structural ceiling in the facility obvious to the casual observer?

[21] Schaub JL, Biery Jr KD. *The ultimate security survey*. Butterworth-Heinemann; 1994 (Updated 2016).

Ensure whether service entrances are protected. Are there:

1. Roof hatches?
2. Ventilation ducts?
3. HVAC openings?
4. Elevator service doors?

29. INTERIOR BUILDING DESIGN: A CHECKLIST

1. Where is the security office and where is the human resources office?
2. Examine security as it pertains to cash and the storage of cash overnight.
3. Be familiar with cars parking within the complex.
4. Examine all interior and exterior doors, door hardware, and door design. Check interior and exterior lighting levels. Check intercom systems, alarms, as well as interior and exterior video surveillance systems.
5. Is there a clean desk policy for confidential documents and are desks and file cabinets all locked at night?
6. Visitors:
   a. Are they restricted as to how far they can maneuver?
   b. Are there assigned elevators?
   c. Is there limited access?
7. What are the provisions and placement of the reception/customer service desk?
8. Where is the vulnerable equipment and stock housed?
9. Custodial quarters:
   a. Where will it be housed?
   b. Where are the master keys kept?
10. How secure is the data center?
    a. What other security devices will be installed?
    b. Can this area be secured when the staff leaves at night?
11. Can the staff areas be properly secured?
    a. Industrial plans should be designed and laid out to combat internal vandalism.
12. Electric, water, and gas meters should be built into the outside wall for service access.
13. Are buildings that are accessible to public use, in addition to shape and layout, designed with deterrents to prevent crime?
14. Is there access for handicapped and disabled people and for individuals with special needs?
    a. Designated parking areas
    b. Guard rails
    c. Telephones
    d. Toilets

15. Is their adequate lighting 24 h a day?
16. Are there provisions for one-way mirrors (retail and high-theft areas)?
17. Digital video surveillance system (CCTV):
    a. Who will monitor it?
    b. ls it integrated with the intrusion detection system with digital recording and storage devices?
18. Will walkie-talkies, radios, or cell phones be utilized?
19. Is there a zoned intrusion alarm panel at the street level for quick police response?
20. Is there a zoned fire alarm panel at the street level for quick fire department response?
21. Is freight elevator access to the dock area or street level secured during nonoperational hours?

30. EXTERIOR BUILDING DESIGN: A CHECKLIST

1. External doors
    a. Type (steel doors and frames) and placement of exit doors.
    b. Design and strength of door and frame.
    c. Choice and strength of panels: glass and wood.
    d. Nonremovable hinges.
    e. Minimum number of entrances, but many exits.
    f. Secure fire doors.
    g. Secure tools and ladders in overhead door locations.
    h. Lighting over entrances.
    i. Quality locks and hardware (latches and bolts).
    j. Minimum exterior hardware on egress doors wherever possible.
    k. Recessed magnetic contacts on alarmed doors.
    1. Panic hardware for quick exit during an emergency.
    m. Kick plates.
    n. Door stops, closers, and holders.
    o. Weather stripping.
2. Building line
    a. Line of sight and natural surveillance.
    b. Bushes less than 3 ft tall at hidden entrances.
3. Check for architectural defects affecting security
4. Roof
    a. Alarmed access to roof or roof hatch.
    b. Skylights.
    c. Pitch angle of roof.
5. External pipes: flush or concealed
6. Podium blocks: access to upper windows

7. Basement area
   a. Access points inside and out.
   b. Storage areas.
   c. Lighting.
   d. Fuel storage areas.
   e. Number of entries to basement, stairs, and elevator.
   f. Grills on windows.
   g. Level of security for your telephone lines and PBX system.

31. SIGNAGE[22]

There are four basic types of signage:

Informational signs: for example, a sign pole may be utilized to locate a destination and/or orientate the individual in the built environment.

Directional signs: where information is displayed to find destinations that may be located in several strategic points in the built environment.

Identification signs: where information about individual locations is displayed such as buildings, locations, and public facilities.

Warning signs: to indicate safety procedures such as emergency exits, no smoking areas, loading zones, and pedestrian crossings.

Signs should be plainly displayed and be legible from a reasonable distance. The size and coloring of the signs, the lettering, and the interval of posting must be appropriate to the situation.

SIGNAGE: SECURITY APPLICATIONS AND CPTED[23]

Well designed, strategically located signs and maps contribute to a feeling of security. Signs should be standardized to give clear, consistent, concise, and readable messages from the street. Having addresses lit up at night will make them even more visible. Where it is difficult to find one's way around, signs with maps may help. Signs must be visible, easily understood, and well maintained. Graffiti and other vandalism can make signs unreadable. If signs are in disrepair or vandalized, it gives an impression of lack of ownership and thus adds to a sense of fear.

Signs should be large, legible, and identifiable. The use of strong colors, standard symbols, simple shapes, and graphics is recommended for signs for restrooms, telephones, information, and help.

Signs should convey the message with adequate information. For example, the signage should indicate where to go for assistance or help, where the telephones and restrooms are, or what are their hours of operation.

The message should be conveyed in suitable language(s) or pictographs.

[22] *Army Field Manual, No. 3–19.30.* Headquarters Department of the Army, Washington, DC; 8 January, 2001. p. 9.
[23] http://www.popcenter.org/tools/cpted/PDFs/NCPC.pdf.

Signs should be strategically located at entrances and near activity areas (e.g., intersections of corridors or paths) and placed for visibility at an appropriate height.

Signs should be maintained on a regular basis to ensure that they are visible. This may involve trimming any landscaping growth or cleaning the sign.

In large parks and buildings, maps or leaflets containing information appropriate to the different needs of various groups of users should be available.

The hours of operation and when exits are closed should be indicated at all perimeter entrances.

CONTROL SIGNS

Signage should be posted where necessary to assist in control of authorized entry, to deter unauthorized entry, and to preclude accidental entry.

WARNING SIGNS

There must be a system in place to warn intruders that the area is restricted. Warning signs should be installed along physical barriers of an area and at each entry point so they can be seen readily and understood by anyone approaching the perimeter. In areas where English is one of two or more languages commonly spoken, warning signs must contain the local language in addition to English. Warning signs must be positioned on or outside the physical barrier area and should be at intervals of no more than 100 ft.

Signs must not be mounted on fences equipped with intrusion detection alarm equipment because nuisance alarms could be caused by environmental movement of the signs. Additionally, the restricted area warning signs must be posted at all entrances to limited and exclusion areas.

OTHER SIGNS

Signs setting forth the conditions of entry to an installation or area should be plainly posted at all principal entrances and should be legible under normal conditions at a distance not less than 50 ft from the point of entry. Such signs should inform the entrant of the provisions of search of the person, vehicle, packages, etc., or prohibitions (such as against cameras, matches, lighters, entry for reasons other than official business).

32. TYPES OF DOORS

PHYSICAL ENTRY AND ACCESS CONTROL DOORS

Personnel doors in both exterior and interior building walls may be single, double, revolving, sliding, or folding. In a normal security setting, their function is to provide a barrier at a point of entry or exit. In a high-security setting,

a door must offer the maximum delay time before penetration by extraordinary means.[24]

Hollow core: made from thin sheets of wood veneer glued over a wood frame with a cardboard insert.

Solid wood/solid wood core: made from solid wood or wood veneer that is glued over a solid wood door.

Metal: made from either galvanized Zintec or a thin, metal sheet of steel that glued over a solid wood door.

Doors can be weaker or stronger than the door frame. Hinges and hinge pins can be defeated. Measures can be taken to strengthen the doors by adding a steel plate for reinforcement, anchoring frames, adding kick plates, or using set screws in hinges or spot welding hinges.

Vehicular doors may be single, double, hanging, rolling, or folding. They can usually be penetrated with hand tools or vehicles. They can also serve secondarily as passageways for personnel. As with any large opening, vehicular doors create a vulnerability of unrestricted pedestrian access.

Exterior doors: All exterior doors, except sliding doors or metal doors, with or without decorative moldings, shall be either solid core wood doors or stave or solid wood flake doors and shall have a minimum thickness of 1¾″ in.

1. *Hollow core doors*: no hollow core door or hollow core door filled with a second composition material, other than the ones mentioned earlier, will be considered a solid core door.
2. *Hinges*: all exterior door hinges shall be mounted with the hinge on the interior of the building. Except where a nonremovable pin hinge or stud bolt is used, such hinge may be installed with the hinge facing the exterior of the building.
3. *Hinge and strike plate lock area*
   a. The shim space between the door buck and door frame shall have solid wood filler, 12 in. (12″) above and below the strike plate area to resist spreading by force applied to the door frame.
   b. Screws securing the strike plate area shall pass through the strike plate and door frame and enter the solid wood filler a minimum of 1/4″.
4. *Glass in exterior doors*
   a. No glass may be used on any exterior door or window within 40″ of any lock except:
      i. That glass shall be replaced with the same thickness of polycarbonate sheeting of an approved type. *Note*: plexiglas shall not be used to replace glass.
      ii. That door locks shall be a double cylinder keyed lock with mortised dead bolt that extends into the strike plate a minimum of 1″.

[24] Fennelly LJ, Perry M. *Effective physical security*, 5th ed. Elsevier, Cambridge, MA; 2017 (Approaches to Physical Security, Chapter 6).

   b. French doors shall have a concealed header and threshold bolt in the stationary or first-closed door, on the door edge facing. The first area of concern with double doors is to ensure that one door is braced to reduce the inward give of the doors. This leaves only one door active. You can make wooden doors stronger by fitting a steel strip and plates to the door frame and around the lock. Fit bolts to the top and bottom of French doors.
   c. Dutch doors shall have a concealed header-type securing device interlocking the upper and lower portions of the door in the door edge on the door strike side, provided that a double cylinder lock with a 1″ dead bolt be provided on the upper and lower sections of the door and the header device be omitted.

5. *Sliding glass doors*
   a. Sliding glass doors shall be installed so as to prevent the lifting and removal of either glass door from the frame from the exterior of the building. To stop the door from being lifted out of its frame, the "jimmy-plates" or screws should be mounted at the top of the track to reduce any vertical play in the door.
   b. Fixed panel glass door (nonsliding) shall be installed so that the securing hardware cannot be removed or circumvented from the exterior of the building.
   c. Each sliding panel shall have a secondary locking or securing device in addition to the original lock built into the panel.
      Secondary device shall consist of:
      i. A "charlie bar"-type device (A "charlie bar" folds down horizontally and blocks movement of the sliding portion of the door. This type of locking device has the advantage of high visibility, which may deter a potential intruder and is also easy to install.
      ii. A track lock, wooden or metal dowel placed in the door tracks
      iii. Inside removable pins or locks securing the panel to the frame
   d. All "glass" used in exterior sliding doors and fixed glass panels to be of laminated safety glass or polycarbonate sheeting. Plexiglas or single-strength glass will not qualify for this program.

How to secure doors that have glass panels:

1. Install a clear, unbreakable polycarbonate panel over the glass on the inside of the door or use the pane to replace the existing glass. Fasten the panel securely on the inside of the door.
2. Install grated wire mesh, a wrought iron grille, or decorative wire grate over the glass. Make sure there is no access through the grate.
3. Install a clear antipenetration film over the glass.

Pet doors: convenient, but may be an easy point of entry for a burglar.

Garage doors: if you use an automatic door opener, change the code from the factory setting. When you go on vacations, disable the opener and place a padlock through the track.

Storm door: offer minimal security protection—cannot rely on for security unless they are reinforced with steel and deadbolt lock.

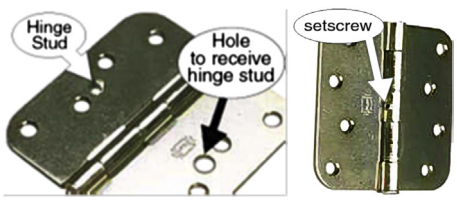
33. DOORS AND DOOR FRAMES[25]

Make sure the doors and frames are strong and in good condition. Exterior wooden doors should be solid and at least 44 mm (1¾″) thick. Fit deadlocks to all outside doors, including French doors. All the exterior doors should have equal resistance to forced entry. The front door is the most obvious, usually the easiest to get to, and is the first one tried by a burglar. The quality of the door is equally important as the lock installed. Steel doors or solid core wooden doors provide satisfactory resistance against forced entry. Any hollow core door should be replaced or at least reinforced by adding exterior-grade plywood on the outside of the door. A hollow core door is filled with corrugated cardboard and is easily broken through. A stile and rail door has stiles and rails as part of the face of the door; the remainder is composed of inset glass or wooden panels that can easily be forced.

The panel edge is the weak point in a stile and rail door and should be reinforced with exterior-grade plywood[26].

EXPOSED HINGES[27]

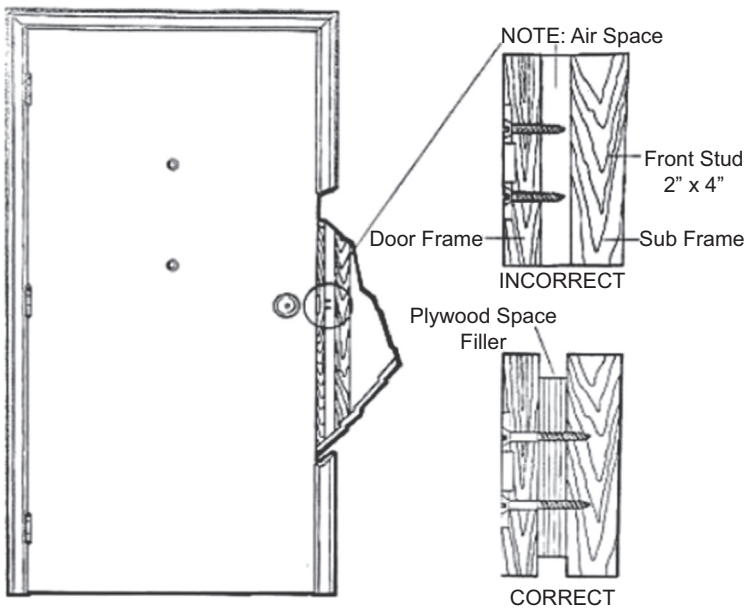
If the door opens outward, you must make sure that your exposed hinges are secured. If exposed hinge pins can be removed, then an intruder can gain entry by swinging the door on the lock after prying open the single hinge.



There are two options for exposed hinges:

- Drill a matching hole in each side of the hinge or remove a matching screw from each. In one hole, insert a screw that is 1/2″ longer than the depth of the hole. Cut off the screw head so that when the door closes, the headless screws will fit into the hole on the opposite side of the hinge and hold the door to the frame even with the hinge pin removed.
- To prevent hinge pins from being removed, drill a small hole into the hinge and insert a small steel pin or screw to hold the pin in place so it cannot be removed.

[25] National Crime Prevention Institute, Louisville, KY; 2010.
[26] http://www.dricon.com/.
[27] https://learningcenter.statefarm.com/residence/safety-1/door-hinges-and-home-security/.



Door Frames and Subframes

The door frame is the decorative soft wood, usually 3/4" thick, that surrounds the door, often with an air space between the frame and subframe, which consists of 2" X 4"s. It is not unusual for 3/4" screws to be used to attach the hinges and strike plates of a door to the frame.This allows a strike plate to give way and entry to be gained.

Measures can be taken to reinforce the frame. Check to see if there is an air space between the frame and subframe. If there is, fill that space with a piece of plywood that needs to extend only 2 or 3 inches above and below where any screws will be attached to the frame.

Then use 3-inch fully threaded screws to secure the strike plate and hinges to the frame. This will anchor the hardware to the subframe and effectively enhance its ability to withstand force (see diagram).

National Crime Prevention Institute (2010).

STRIKE PLATES[28]

[28] http://www.grainger.com.

A strike plate comes with every door lock. Many times these strike plates are cosmetic and not intended to provide much security. The strike plate's attachment to the door frame is usually the weakest point in the entire door/door frame/lock system.

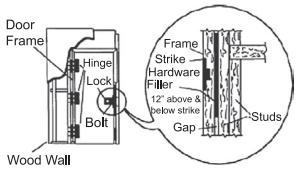
High-security strike plates are available. They sometimes come with a heavy gauge metal-reinforcing plate that mounts under the cosmetic strike plate and come with 3″-long screws that secure the strike to the wall framing, not just to the door frame jamb.

The screw holes are staggered so the screws do not penetrate into the same grain of wood. The concept of screwing into different wood grains in the door frame and wall framing is to make it more difficult to split the wood door frame or wall framing when the door is impacted. This should be considered for every exterior door and at doors coming from attached garages.

DOOR FRAMES[29]

Locks can be defeated by a method known as "spreading" where a wedge or jack-like device is inserted in-between the two door frames. Spreading can be successful because doors and frames are purchased as single units and are placed into the wall opening during construction. Even though the opening between the wall and the frame is braced at the top and bottom with wedges, the middle of the door/door frame is often left unsecured, which permits the frame to bow under pressure. Solid blocks inserted between the openings will help to resist "spreading."

To strengthen the frame, install four, 4 in. screws through the doorstop strip and the frame and into the stud of the wall construction, about 4 and 12 in. above and below the strike plate. The same thing can be done to the hinge side of the door to further reduce the "spreading" of the door frame.



A metal plate can also be installed on the inside of your door frame, surrounding the strike plate opening. This plate will help reinforce the door frame at its weakest point.

DOOR VIEWERS

All exterior doors should have a door viewer (peephole) with a 180-degree field of view, unless there is a window for seeing who is outside the door before it is opened.[30]

How to Lock out Crime, CMHC, 2007. How to Lock out Crime has been out of print for some time and may contain outdated information. CMHC assumes no responsibility for the use of or any damages suffered by the Client or any third party as a result of the use of the information contained in the Publication.

[29] Fennelly LJ. *Effective physical security*. Elsevier, Boston, MA; 2013.
[30] https://www.canada.ca/en/services/policing/police/crime-and-crime-prevention.html.

EXTERIOR DOORS IN COMMERCIAL OR BUSINESS APPLICATIONS

- Doors should be numbered on the interior and exterior (using clockwork numbering) so that they can be easily identified in the event of an emergency.
- So that people accessing the building can be directed to the appropriate entrance/exit, exterior doors should have signage indicating whether the door is to be used for emergency exit, employee entrance, authorized personnel only, visitor entrance, etc.

34. DOOR MANAGEMENT[31]

Door management products are compatible, complementary components to any access control system. They can enhance the level of security at any door and are visually as unobtrusive as a thermostat on the wall.

No matter what access control system is used by the facility, door propping (creating unauthorized entry/exit points) and "tailgating" behind authorized card holders are common problems that cause security personnel to be constantly dispatched for nuisance alarms. Door management products were born out of the need to help resolve these common access control issues.

The units can be used to activate peripheral devices, such as dialers, door locks, and cameras, and can be keyed to match a building management's master key system.

DIGITAL VOICE ALARMS

The digital voice alarm, used as a stand-alone device or tied to access control systems, combines door prop monitoring with high-quality studio digitally recorded voice messages, such as:

- "This exit is for emergency use only."
- "This door is in alarm mode. Please close the door."
- "Please enter your personal identification number."
- "Access is denied. Proceed to the security office."
- "Caution. Vehicle traffic approaching."
- "Please return badge to the security office."

This unique and effective security solution encourages users to keep monitored doors closed, which reduces nuisance alarms. Users are given verbal warnings before an alarm is activated, with an adjustable warning period of 0–90 s.

SAMPLE APPLICATIONS

- Lobby, reception, and executive office environments; doors propped by smokers; and retail antitheft doors.
- Integrated with motion detectors: direct individuals away from emergency-use-only exits.

[31] Permission obtained to reproduce from Designed Security Inc. Bastrap Texas, 78602.

- Integrated with optical turnstiles: direct users to security office after being denied access.
- Integrated with antitheft doors: announce waiting period for time delay; crash bar exits.

Customized and in-stock messages are available. Your personalized messages can also be recorded.

DOOR PROP ALARMS

The door prop alarm, used as a stand-alone device or tied to any access control system, provides a unique solution to the common security problem of doors being propped or held open. An audible alarm sounds, alerting the user that a violation has occurred before the door-held alarm is issued. This encourages users to keep secured doors closed while reducing the number of nuisance alarms for security staff, provides local and remote identification of security breaches, and has an adjustable time delay of 0–30 s.

DOOR MANAGEMENT ALARMS

Door management alarms (DMAs) complement card reader and access control systems. Monitored doors can remain unlocked, as authorized card swipes deactivate the alarm, not the lock. DMAs provide complete monitoring of access control points by offering door-prop/door-held and intrusion/door-forced detection. It flexibly interfaces with electric locks, produces audible warnings, and reduces nuisance alarms by encouraging user compliance with access control procedures.

EXIT ALARMS

The exit alarm, used as a stand-alone device or tied to any access control system, monitors secured doors. An audible alarm sounds locally for exit violations and for intrusion/door-forced detection. It monitors the door position and activates a high-level sounder and alarm contact when a violation occurs. The alarm can be reset or disabled by a local or remote key switch.

35. MODEL DOOR NUMBERING SYSTEM[32]

EXTERIOR NUMBER POSITION

- All numbers should be placed at the top right of the door.
- Where a multiple bank of doors (3 or more) is present, it is good practice to center the number or put the same number at both ends of the bank.

[32] http://www.nj.gov/education/schools/security/resources/DoorNumbering.pdf.

- Each door may be numbered separately, as follows: 3-1, 3-2, etc.
- Some facilities/organizations choose to mark each door with an individual number when they face different directions (north and east).

EXTERIOR NUMBER SIZING

According to the International Fire Code § 505 requirements, all numbers should be of the correct size in correlation with how far from the street or fire department access it is [Ord. 2010–17 § 1 (part), 2010; Ord. 2007–15 § 1, 2007].

- Structures up to 36 ft away: numbers are a minimum of 4 in. high and a minimum of 0.5 in. stroke width.
- If the structure is 36 to 50 ft away: numbers are a minimum of 6 in. high and a minimum of 0.5 in. stroke width.
- When the structure is more than 50 ft away: numbers are a minimum of 9 in. high and a minimum of 1 in. stroke width. Some facilities/organizations have chosen to use 12 in. numbers for increased visibility. Obviously the larger the number, the greater the distance up to which it will be visible by responders.

36. BUILDING ACCESS: WINDOWS, GLASS, AND SECURITY

The purpose of the window, aside from esthetics, is to let in sunlight, to allow visibility, and to provide ventilation.

The following types of windows provide 100% ventilation:

- Casement
- Jalousie
- Awning
- Hopper

The following types of windows provide 50–65% ventilation:

- Double-hung
- Sliding

Factors to be considered in the selection of type and size of a window are:

1. Amount of light, ventilation, and view requirements
2. Material and desired finish:
   a. Wood
   b. Metal, aluminum, steel, stainless steel
3. Window hardware
   a. Durability
   b. Function

4. Type of glazing available
5. Effectiveness of weather stripping
6. Appearance, unit size, and proportion
7. Method to open, hinge or slider, and choice of line of hinges
8. Security lock fitting
9. No accessible louver windows
10. Ground floor or lower windows—fixed glazing and small openings
11. Consideration of size and shape to prevent access
12. Consideration of size because of cost due to vandalism
13. Use of bars or grilles on inside
14. Glass
    a. Double glazing is a deterrent
    b. Types of glass, tempered glass, laminated, wired, bullet resistant, plated
    c. Vision requirements
    d. Thickness
    e. Secure fixing to frame
    f. Laminated
    g. Use of plastic against vandalism
    h. Fixed, obscure glazing for houses and garages
    i. Shutters, grilles, and louvers can serve as sun control and visual barriers as well as security barrier
15. Plastic
    a. Polycarbonate
    b. Acrylic

TYPE OF WINDOWS

1. *Double-hung wood*: upper outside sash that slides down and a lower inside sash that slides up.
    a. All locking devices to be secured with 1/2 in. fully threaded screws.
    b. All window latches must be key-lock or a manual (non-spring-loaded or flip-type) window latch. When a non-key-locked latch is used, a secondary securing device must be installed. Such secondary securing device may consist of:
        i. Holes drilled in at two intersecting points of each inner and outer window and appropriate-sized dowels inserted into the holes. Dowels to be cut to provide minimum grasp from inside the window.
        ii. A metal sash security hardware device of approved type may be installed in lieu of doweling. Note: Doweling is less costly and of a higher security value than more expensive hardware.
2. *Sliding glass windows*
    a. Horizontal slider window: may have one or more fixed panels in addition to one or more panels that slide on horizontal tracks. Only half of the total window can be opened at one time.

3. *Awning windows—metal windows*
   a. Awning window: similar to a horizontal, top-hinged casement. It tilts out at the bottom, offering partial ventilation and an unobstructed view.
   b. No secondary device is required on awning-type windows, but crank handle may be removed by the owner as security feature.
   c. Double-hung metal windows are secured similar to the double-hung wood window using metal dowels.
4. *Bay window*: projects out from the wall. There is a center window parallel to the wall that is flanked by two windows, usually casement or double-hung style, that are attached at an angle. Box bay windows have side windows at 90-degree angle.
5. *Bow window*: projects like a bay, but has more than three sections that join to form a gentle curve. Center windows are generally fixed and side sashes are typically casement windows.
6. *Hopper window*: similar to an awning window, except it opens at the top instead of the bottom for partial ventilation.
7. Jalousie window: also called louvers and are made of glass slats set in metal clips that can be opened and closed in unison.
8. *Fixed frame*: stationary windows that are inoperable, do not open or close.

Windows that are larger than 96 square inches or that are less than 18 ft off of the ground or less than 14 ft from trees, poles, or adjoining buildings should be protected.

STEEL SECURITY SCREENS, GRILLES, OR BARS

If heavy, security screens, grilles, or bars are utilized on the interior or exterior of windows, there should be an emergency release on the inside of the window for emergency exit.

WINDOW GLASS/GLAZING

Six types of window glass or glazing are:

1. *Sheet glass*: least expensive and the most vulnerable to breakage.
2. *Plate glass*: e.g., mirrors.
3. *Float glass/annealed glass*: has the quality of plate glass combined with the lower production cost associated with sheet glass manufacturing and is virtually free distortion and defect.
4. *Tempered glass*: treated to resist breakage and is 3–5 times stronger than sheet glass and maybe required by building codes.
5. *Laminated glass*: a type of safety glass that holds together when shattered, when laminated glass is broken, polyvinyl butyral or similar substance is used to hold together the layers of glass.
6. *Bullet-resistant glass*: constructed using a strong, transparent material such as polycarbonate thermoplastic or by using layers of laminated glass. The polycarbonate layer is often sandwiched between layers of regular glass, and since the glass is harder than the plastic, the bullet is flattened and prevents penetration.

ShatterGARD[33] – is a product that increases the structural integrity of any window and offers safety and security by using a film that is applied to glass to increase the overall strength of the glass surface. The film is virtually undetectable to the human eye. Glass films such as ShatterGARD reduce the need for security screens, grilles, or bars.

SECURING WINDOWS WITH LOCKS

- *Window sash locks*: found on wooden, aluminum, and vinyl windows. Most sash locks have a 1-in. wide base to accommodate standard window frames. Some types have a thumb turn and some are operated with a key.
- *Steel pins*: inserted in a drilled hole through both sections of the window to prevent prying or lifting. Steel pins can also be used on sliding patio doors.
- *Twist-in lock*: used in the track of a sliding windows (and doors) door to secure it in a closed or ventilating position with a bolt that is tightened by a thumbscrew or a key. When the bolt is thrown, it prevents the window (or door) from sliding or being lifted off of its track.

37. PRIMARY LIGHTING SOURCES[34]

LED: one of the newest light sources where light is emitted from a semiconductor. It has a greater resistance to shock, vibration, and wear so its life span is increased significantly. It has the potential of furnishing a cost-effective alternative that lasts longer without sacrificing illumination.

Incandescent: the least efficient and most expensive lighting to operate and it has a very shout life span.

Fluorescent: more efficient than incandescent lamps, but are not used extensively outdoors. Inefficient in cold weather, but have a long life span. Slowly being replaced by energy-saving LED units.

Halogen and quartz halogen: provides 25% better efficiency and life than ordinary incandescent bulbs.

Mercury vapor: takes several minutes to produce full light output, but has a long life.

Metal halide: imitates daylight. Works well with video surveillance, but expensive to install and maintain.

High-pressure sodium: energy efficient and have a long life.

Low-pressure sodium: more efficient than high-pressure sodium, but are expensive to maintain.

Induction: have a long life and are similar to fluorescent lamps.

Infrared: invisible to the naked eye, but may be useful for video surveillance illumination.

[33] http://www.shattergard.com.

[34] Fennelly LJ. *Handbook of loss prevention and crime prevention*, 5th ed. Elsevier, Boston, MA; 2012.

FORMULA TO DETERMINE THE COST A LIGHT SOURCE[35]

Watts (on the bulb or light source) × hours = Watt hours
Watt hours/1000 = Kilowatts
Kilowatts × rate (on the electric bill) = Cost

38. ILLUMINATION

- *Illumination intensity*: as light bulbs age, the light that they emit decreases. Some objects and colors reflect light better than others, and this affects the intensity.
- *Illumination distribution*: lighting fixtures have to be spaced correctly so that there is no area without proper illumination.
- *Illumination quality*: color perception may or may not be important. This may affect the quality of video surveillance.
- *Illumination reliability*: may be a problem if the lights are vulnerable to physical attack or vandalism.[36]

Lighting and the intensity of illumination falling on a surface is measured in foot candles (fc), which are English units, or lux, which is a metric unit, and a general rule is that "at night, outside of a building or at a parking lot, one should be able to read a driver's license or newspaper with some eyestrain".[37]

One foot candle equals one lumen of light per one square foot of space. One lumen is the measure of light at its source and the amount of light needed to light an area of one square foot to one candlepower.[38]

39. SEVEN BASIC TYPES OF PROTECTIVE LIGHTING[39]

PROTECTIVE LIGHTING

Lighting is the single most cost-effective deterrent to crime. An illuminated area acts as a psychological and physical deterrent, and it can reduce criminal opportunity. Research shows that there is a close relationship between crime/the fear of crime and illumination. Lighting is a powerful tool for crime prevention by enhancing safety and may possibly reduce potential liability.

The seven basic types of protective lighting are:

- *Continuous lighting*: fixed and the most common type of lighting in which lights are installed in a series to maintain uniform lighting during hours of darkness. These lights are frequently set on timers or controlled by sensors.

[35] http://www.lightsearch.com/resources/lightguides/formulas.html.
[36] www.asisonline.org/poa.
[37] L. Fennelly. *Handbook of Loss Prevention and Crime Prevention*, 5th ed. Lighting Chapter. Elsevier, Boston, MA; 2012.
[38] Fennelly LJ. *Handbook of loss prevention and crime prevention*, 5th ed. Elsevier, Boston, MA; 2012.
[39] Ibid.

- *Standby lighting*: turns on with alarm activation or when suspicious activity is suspected.
- *Moveable lighting*: manually operated search lights
- *Emergency lighting*: can duplicate other lighting systems in the event of an emergency. Use is limited to times of power failure and other emergencies. Emergency lights usually depend on an alternative power source.
- *Controlled lighting*: used outside a perimeter to illuminate a limited space.
- *Area lighting*: used in open areas and parking lots.
- *Surface lighting*: used on the surface of structures and buildings.

40. SECURITY LIGHTING[40]

LIGHTING REQUIREMENTS

Each organization should ensure a minimum level of light for their respective property areas that complies with all applicable regulations and industry guidelines. Security lighting requirements should be specified by a lighting engineer. Ideally, lighting requirements will be identified as part of a security survey. The lighting program should take account the following:

- Lighting should not illuminate security/protection officers or patrols. Where security patrols cannot be kept out of the zones of illumination, a judgment must be made between the advantages of the lighting and the reduction in patrol effectiveness.
- Lighting must be combined with surveillance. The deterrent effect of lighting depends on the fear of detection. This may also require video surveillance or security/protection officers on static posts and mobile patrols.
- Lighting must not cause nuisances or hazards to neighbors, such as light pollution or light trespass. Lighting may adversely affect adjoining or adjacent properties such as residential properties, roadways, airports, harbors, neighboring commercial buildings, or properties.
- Lighting must be cost-effective and compatible with site conditions. It may not be economical to illuminate very large areas. Take into account both the existing lighting outside the perimeter and the lighting installed within the site for operational or safety purposes.

LIGHTING SYSTEMS

The basic systems of security lighting that may be used either singly or in combination are: perimeter lighting, area lighting, and floodlighting. Other forms of lighting may also be required, such as gatehouse lighting and topping-up lighting.

[40] Fennelly LJ. *Handbook of loss prevention and crime prevention*, 5th ed. Elsevier, Boston, MA; 2012.

PERIMETER LIGHTING

Perimeter lighting is used to illuminate the property line or fence itself and an area beyond (i.e., the detection zone). When used with chain-link fencing, a narrow strip inside the fence is also illuminated. When double fences are used, the detection zone lies wholly or mainly between the two fences.

The objective is to reveal an intruder's approach and produce glare toward him, thus reducing visibility into the site. It may therefore be suitable for use with patrolling guards. However, it can be difficult to apply because it may create nuisance or hazard or because of a lack of sufficient open flat ground outside the perimeter.

AREA LIGHTING

Area lighting is used to illuminate the area within the perimeter that an intruder must cross to attack the target. The goal of area lighting is to produce even illumination without dense shadows.

Guardhouse lighting is used at perimeter entrances and guardhouses to:

- Reveal approaching vehicles and pedestrians and allow security/protection officers to identify them, verify entry, and carry out vehicle searches.
- Conceal security/protection officers within the guardhouse while allowing them to see out.

FLOODLIGHTING

Floodlighting is used to cast a strong light on the walls of buildings so that intruders are visible either in silhouette or by the shadows they cast.

LIGHTING EQUIPMENT AND SYSTEM DESIGN

The detail design of the system and choice of equipment must be carried out by a qualified lighting engineer who must be briefed regarding the site requirements. Take into account the following points:

CONTROLS

Automatic control of lights by photoelectric cell is often convenient, compared with timers that need to be set, but manual override at a central control point may be required to switch off all, or selected parts, of the system. Switching on lights in response to a signal from an intruder alarm, although economical in running costs, is of doubtful value.

WIRING

Electrical supply cables to lights should be buried; where unavoidably exposed, they should be armored or contained in steel conduit.

41. GOALS OF SECURITY LIGHTING

1. *Objective illumination*: will allow observation of the protected item.
2. *Physical deterrence*: uses a sufficient light level to cause psychological responses such as pain and temporary blindness. The light source can be continuous or event-responsive and 100,000 fc will cause temporary blindness for 2–3 min.
3. *Glare projection*: achieved by projecting light away from the protected property so that an approaching intruder cannot see onto the premises, but they are highly visible from the inside.
4. *Psychological deterrence*: results when lighting leaves potential intruders fearful that they will be detected, identified, and/or apprehended.

42. LIGHTING RECOMMENDATIONS

ILLUMINATION LEVELS

- *Horizontal illuminance*: measured at grade level with the light meter placed on horizontal surface, such as the pavement.
- *Vertical illuminance*: measured 5 ft above grade with the light meter also at 5 ft above grade. Vertical illuminance should be provided where there is a need to identity the face and body of people, at a distance of 30 ft. There should be a uniformity ratio of no more than 4:1 variance in lighting. The higher the background illuminance, the higher the vertical illuminance must be to maintain the 4:1 ratio to prevent silhouetting.

RECOMMENDED ILLUMINATION LEVELS

Outdoors[41]

- Perimeter or outer area 0.15 fc
- Perimeter of restricted area 0.4 fc
- Vehicular entrances 1.0 fc
- Pedestrian entrances 2.0 fc
- Sensitive area 0.15 fc
- Sensitive inner structure 1.0 fc
- Entrances 0.1 fc
- Open yards 0.2 fc
- Perimeter fencing 0.5 fc

Indoors[42]

- Hallways and corridors 5.0 fc
- Exit ways 5.0 fc

[41] Fennelly LJ. *Handbook of loss prevention and crime prevention*, 5th ed. Elsevier, Boston, MA; 2012.
[42] www.osha.gov/cfr1926.56.

- Restroom 10.0 fc
- Mechanical/electrical room 10.0 fc
- Offices 30.0 fc

The following recommended illumination levels were taken from the *Illuminating Engineering Society of North America IES Handbook*, Ninth Edition.

Recommended Illumination Levels for Example Areas or Locations	Recommended Horizontal fc	Recommended Vertical fc
Facial identification	N/A	0.5–0.8 fc
Parking facilities on pavement	6 fc	0.5–0.8 fc
Parking facilities gathering points	5 fc	0.5–0.8 fc
Parking lots open spaces	3 fc	0.5–0.8 fc
Parking lots likely loitering areas	1 fc	0.5–0.8 fc
Park trails and walkways	0.6 fc	0.5–0.8 fc
Major retail parking lot	3 fc	0.5–0.8 fc
Major retail low activity—entrance	5 fc	0.5–0.8 fc
Convenience/gas station pump	6 fc	0.5–0.8 fc
Convenience sidewalks and grounds	3 fc	0.5–0.8 fc
Convenience store interior	10 fc	0.5–0.8 fc

43. TWENTY SIMPLE WAYS TO SAVE ENERGY (LEED)

LEED is an acronym for Leadership in Energy and Environmental Design. It designates environmentally responsible—sometimes referred to as "green" or "sustainable"—commercial buildings designed, built, and operated to optimally use the building location, minimize nonrenewable energy use, and reduce water consumption, while offering healthy settings in which to work and live.[43]

1. Use LED lighting that lasts longer, burns brighter, and consumes less energy. Energy-efficient bulbs like LEDs consume 25–80% less energy compared with traditional incandescent bulbs. Switching to LED bulbs is a great way to save money and energy.
2. When installing/using LED lighting, it is important to:
   a. Use nonglare fixtures.
   b. Ask about who manufactured these devices and use only the quality products.
   c. Ask about the age of the fixture you are installing.
3. For energy efficiency, have a motion detector turn on lights in restrooms.

[43] http://leed.usgbc.org.

4. Utilize timers or photoelectric cells to control exterior lighting.
5. Develop a recycling program to properly manage waste, for example, cans, plastic, light bulbs, paper, cardboard, wooden pallets, as well as electronic waste.
6. Use Energy Star-labeled products.
7. Unplug appliances and machinery that are not in use. The Lawrence Berkeley National Laboratory found that some devices can use as much as 20 W of power when they are turned off, but not unplugged.
8. Consider the use of solar systems and/or wind power to improve your power needs.
9. Insulate all hot water pipes.
10. Tint all glass windows.
11. Perform routine maintenance on generative motors, such as those on elevators controls.
12. Insulate all hot water pipes.
13. Design the view from the inside to the outside with maximum visibility.
14. Utilize centrifugal chillers for heating and cooling to improve efficiency.
15. Install trees on the property to provide a degree of shade.
16. Utilize ceiling fans or other strategically placed fans to efficiently move air.
17. Increase efficiency of irrigation systems and/or reduce water flow.
18. Install waterless urinals.
19. Use only "green" cleaning products.
20. Form a partnership with the US Environmental Protection Agency.

Some helpful environmentally responsible or "green" websites are:

www.nrel.gov
www.buildings.com
www.leedonline.usgbc.org
www.pacenow.org
www.wm.comwww.energystar.gov

Your savings on water and energy may equal or exceed your ROI for a LEED investment.

44. EFFICIENT KEY MANAGEMENT: A MAJOR BUSINESS CONCERN FOR THE FACILITY MANAGER

Locks and keys play an important part in managing the day-to-day security of your business; therefore, efficient mechanical key management is a major business concern and a top priority.

In business situations where you need to issue and return dozens or even hundreds of keys, the tracking of keys can become a very time-consuming and difficult task. It is also a necessary task to reduce the risk of loss or theft.

We were involved several years ago in a litigation case of a rape in the apartment complex, and the manager was asked to describe his key control process when a

tenant left and moved on. He said he would open the bottom drawer of his desk and take out a cylinder and rekey the lock from another unit. Sloppy key control does not work. Further investigation proved that the apartments 1, 15, and 21 were all keyed alike.

45. THE BASICS OF AN INTRUSION DETECTION (ALARM) SYSTEM

To determine the type of intrusion detection system that is needed for a home or business, ask the following questions:

- What is the system protecting against?
- What types of sensors are needed?
- Who will respond to the signal transmission?
- How will the signal be sent?

MAIN COMPONENTS OF AN INTRUSION DETECTION SYSTEM

- *Control panel*: the brain of the system and sends an alarm signal when a sensor responds.
- *Keypad or wireless touchpad*: used to arm disarm the system.
- *Sensors*: when a sensor detects a certain condition, the control panel directs the signal.

Alarm signals:

- *Local*: signals an on-site audible alarm.
- *Central station*: signal is sent to the alarm company or a monitoring station.
- *Proprietary*: monitored on-site (usually by security or protection officers).

46. INTRUSION DETECTION SYSTEM: A CHECKLIST

INTRUSION DETECTION SYSTEMS

The intrusion detection system must meet the needs of the facility, operate in harmony with other systems, cannot interfere with business operations, and most importantly, the value of the system is at least equal to the costs of the system.

Deter: The presence of an IDS may deter intruders when signs are posted warning that a site is protected by such a system.
Detect: Most IDS systems are designed to detect an impending or actual security breach.
Delay: When detection occurs, intruders may be delayed or denied by activating other measures.

Respond: IDS systems facilitate security responses by pinpointing where an intrusion has occurred and possibly where the intruder has moved within the site.

THE TYPES OF INTRUSION DETECTION SYSTEM DEVICES THAT ARE USED TO DETECT INTRUSIONS

- Position detection devices: usually a magnet that detects when one part of the device is moved away from the other (door position switch).
- Motion detector: creates an alarm when the static conditions of the protected area change (microwave detectors, passive infrared detectors, ultrasonic detectors, beam detectors, dual technology detectors).
- Sound detectors: transmit an alarm when sounds outside a selectable ambient range are received by the detector (vault).
- Vibration sensors: reacts to motions such as shaking or physical shocks (tool attacks).
- Heat sensors: trigger alarms when the air or surface temperature changes.
- Temperature sensors: trigger alarms when the air or surface temperature changes occur outside of predetermined limits.
- Capacitance devices: detect changes in electrical capacitance (safes and vaults).
- Impact sensors: detect sudden changes in air pressure.
- Glass break sensors: detect the impact that causes glass to break and the sound frequencies of breaking glass or broken glass hitting the floor.
- Duress/panic alarms: employed to protect personnel by transmitting assistance alarms; highest priority level.
- Alarm transmissions, monitoring, and notification media should be supervised to better detect occurrences of tampering or interception. Regular tests/audits should be performed to assure accuracy and timeliness of transmitted information, as well as response by security personnel.
- Intrusion detection sensors can add an extra layer of protection when they are interfaced/integrated with access control, security surveillance systems, lighting, etc.
- Finally, systems should be checked for operation monthly.

47. WHAT IS A SECURITY SURVEILLANCE SYSTEM?[44]

Security cameras are available in a wide range of styles and features, and they are a common component in a security system. Internet security systems or IP cameras use the Internet by networking to send and receive data. They are fairly easy to install and connect to your system, and you can view live camera feeds at any time with free mobile apps for smartphones and tablets. IP cameras can be installed in virtually any location and can monitor the interior as well as the exterior of a facility. Cameras can

[44] https://www.videosurveillance.com/apps/.

also be used to alert security/protection officers to respond to suspicious activities or individuals.

Video surveillance is commonly used for:

Remote video monitoring: to protect against theft, burglaries, and dishonest employees.
Facility protection: to protect the perimeter of the property or the perimeter of buildings.
Monitor operations: to monitor day-to-day operations and as a tool to streamline operations.
Loss prevention: to protect assets.
Vandalism deterrence: visible cameras may be a deterrent to vandals because of the possibility that they can be identified on the video. High-definition cameras with facial recognition in a durable, vandal-proof housing can be used.
Employee safety: for compliance with safety regulations and also to protect the employer in civil proceedings.
Parking lots: to monitor for theft or damage to vehicles as well as accidents.
Event video surveillance: for crowd control as well as crime prevention.
Public safety: routinely used for city streets, parks, communities, and neighborhoods to help deter crime and enhance public safety.
Traffic monitoring: commonly used to improve the flow of traffic and monitor for accidents.
Outdoor perimeter security: security can be maintained in different ways by utilizing video surveillance with security/protection officers on patrol, fences, vehicle, and pedestrian gates and intrusion detection.

48. VIDEO SURVEILLANCE SYSTEMS (CLOSED-CIRCUIT TELEVISION)[45]

Determine the goal of your video surveillance program—whether it is video to be used for forensics (evidence, after an incident) or if a security response will be assessed by the control center operator if he or she observes something or someone that is suspicious. Monitoring and response are vital to a video surveillance program. Video surveillance without critical analysis of the activity that is observed or without a security officer response if one is needed is operationally inadequate. Surveillance monitoring requires all of the following:

- Output from each camera to be displayed at all times unless it can be alarm switched to activate the display when needed.
- Arrangement of the monitor screens to be displayed at all times unless it can be alarm switched to activate the display when needed.

[45] www.asisonline.org/poa.

- A means for bringing any particular camera of immediate interest to a monitor screen in the direct field of view of the camera operator.
- The capability for permanently recording the display from one or more cameras, as needed, and for identifying the recorded material by camera location and clock time.

Each facility should have a video surveillance policy that addresses video surveillance cameras and include the locations and level of critical business needs. Ensure that policies are updated as needed to include a functional purpose of the cameras for the locations of their coverage. This establishes the business purpose and ensures a solid foundation for the application of video surveillance solutions.

To achieve a possible deterrent effect, install clearly visible signage indicating that the area or property is being monitored by video surveillance, especially in the parking garages and surface parking lots.

49. MONITORING IMAGES[46]

Today, far more video is being recorded than anyone could ever monitor or search. Complex surveillance systems monitor not just dozens, but hundreds or even thousands of cameras.

Research from Sandia National Laboratories which develops science-based technologies that support US national security, states that, "…an operator is likely to miss important information after only 20 minutes in front of a monitor; intelligent video can help operators cover more cameras and respond more quickly."

Without some form of built-in algorithm compiling relevant information, there is simply no efficient way to monitor all the surveillance cameras in a video surveillance system.

ISO 11064-4:2013[47] specifies ergonomic principles, recommendations, and requirements for the design of workstations found in control centers. It covers control workstation

[46] www.securityinfowatch.com.
[47] https://www.iso.org.

design with particular emphasis on layout and dimensions. It is applicable primarily to seated, visual display–based workstations, although control workstations at which operators stand are also addressed. These different types of control workstations are to be found in applications such as security installations.

50. VIDEO ANALYTICS AND THERMAL IMAGING CAMERAS[48]

Video analytics (intelligent video) can be utilized to increase productivity and reduce the amount of video surveillance storage. Additionally, security/protection officer performance may be improved and response times reduced, by using video analytics or "intelligent video." This will turn video into "actionable information" for the control center officer, which will allow him or her to receive visual or audible alerts and make decisions regarding appropriate next steps. In this way, cameras are programmed to "standby" and only record when there is motion or activity in a defined area. When the camera begins to record, the control center is notified of a potential problem in that area and can dispatch a security officer/police officer or call 911, if necessary. Security/protection officers at the control center would have the capability to override the video analytics program and manually control the cameras, if necessary. This would help to ensure that control center operators are alert and motivated.

Additionally, an ergonomic console design can be designed to reduce fatigue, eyestrain, and boredom. Sensor alarms or simple switchers can be programmed to call up and display a monitor scene that needs attention. To utilize the full capabilities of the video surveillance program, control center officers could utilize the cameras to conduct "virtual tours" of the campus and document findings.

THERMAL IMAGING

Thermal sensors and cameras create video images from infrared heat waves. Infrared is part of the electromagnetic spectrum with wavelengths that are longer than visible light. The warmer the object, the more energy it emits.

The benefits of utilizing thermal cameras with analytics are:

- Good useable image both day and night and in adverse conditions.
- Reliability of the analytics, as well as visual assessment capabilities of the operator receiving the alarm.
- No lighting required.
- Customers/users may be able to turn off site lighting or minimize it.
- Low power and bandwidth consumption.
- Low maintenance and cost of ownership.

[48] http://www.securitymagazine.com/publications/3.

51. SECURITY/PROTECTION OFFICER OPERATIONS[49]

Security/protection officer functions include:

- Screening employees and visitors in reception areas.
- Controlling the movement of personnel and vehicles in and out of the facility and control the movement of company property.
- Patrolling the company property on foot, in a vehicle or by video, and gather and report information.
- Monitoring video surveillance and life safety systems.
- Responding to security incidents.
- Documenting incidents.
- Escorting visitors.
- Assisting with parking issues.
- Utilize various security measures (doors, locks, alarms, video surveillance, lighting, etc.).
- Security officers must have the complete support of management to enforce company security policies.

Recommended qualifications of a security/protection officer:

- Good character
- Positive attitude
- Professional appearance
- Professional behavior
- Physically Fit

POST ORDERS

Security/protection officer post orders should be kept current, outline the job duties and responsibilities, and describe potential scenarios. We strongly believe that all security/protection officers need to be properly trained. It is important that they know the basics of day-to-day operations as well as what to do in an emergency situation.

Additional information to be included in post orders:

- Date of revision (should not be older than 5 years, at the most)
- Notice of confidentiality
- Emergency contact information (internal and external), including afterhours contact information
- Description of the facility and its users (floor plans, if possible)
- Discussion and review of subjects such as access control, keys, equipment control, property removal, employee, visitor, vendor and contractor procedures, mobile patrols and static posts, as well as general site policies and procedures

[49] Fennelly LJ. *Handbook of loss prevention and crime prevention*, 5th ed. Elsevier, Boston, MA; 2012.

- Specific instructions on the handling of emergency situations
- Security staffing levels, hours of coverage, and specific functions and duties
- Proper operation of all emergency and nonemergency communications equipment
- Instructions on public relations
- Code of ethics and standards of conduct

52. LETHAL AND NONLETHAL WEAPONS FOR SECURITY/PROTECTION OFFICERS

In some locations, security/protection officers carry lethal weapons (firearms). If this is the case, additional training is required—similar to law enforcement officer training, which would include both classroom and firearms qualification courses to meet initial as well as ongoing training requirements.

Most security professionals recommend considering the use of nonlethal tools—such as pepper spray products, batons, TASERs, or handcuffs. Many post order documents state that one of the functions of security/protection officers is to "intervene to protect the physical safety of others and to the extent permitted by law restrain individuals threatening imminent injury to others." The ability of security officers to restrain individuals to protect the safety of others is a fact to be considered when deciding between lethal and nonlethal weapons. For any nonlethal option listed earlier, training would be required.

Regardless of whether the choice is to issue security/protection officers lethal or nonlethal weapons, a Use of Force Policy should be established and documented in the post orders.

53. THE SECURITY/PROTECTION OFFICER'S CHECKLIST

If security/protection officers are needed to protect the site, determine the following:

1. Hours of coverage required.
2. Do they answer to the contract security company or the owner/manager of the property?
3. Are they employees of the contract security company or the facility (proprietary security)?
4. What are their powers (detain, arrest, etc.), if any?
5. How are they supervised? What is the frequency of supervision?
6. What type of training do they receive for this site?
7. Have local police been advised of their presence on site?
8. What is the equipment assigned to the security/protection officer on duty? Flashlight (size), baton, TASER, chemical agents, handcuffs, etc.?
9. What is the total number of officers needed?
10. What keys or access cards to the facility does the officer need for patrols or emergencies?

11. Are there post orders? What are the protection officer's exact duties? Are the posts fixed, or is it a mobile or walking patrol?
12. Review the security officers' patrol procedures.
13. Are the security/protection officers carrying an RFID scanner to scan patrol points or a "pipe" system?
14. Will the officers complete a daily activity report or a "pass-on log" for each shift?
15. Who will review daily activity reports and incident reports?
16. Do the security/protection officers have sufficient responsibilities and are they active throughout their shifts?
17. Do the security/protection officers have an up-to-date list of whom to contact in case of emergency?
18. How will security/protection officers communicate—radio, walkie-talkie, or cell phone?

54. SECURITY/PROTECTION OFFICERS: DAY-TO-DAY OPERATIONS AND DEALING WITH FALSE ALARMS

Security/protection officers who respond to routine and emergency situations are an important link in day-to-day operations. They monitor your communications, video surveillance, radio activity, access control, telephone services, and alarm/fire panels. They are basically your eyes and ears.

FALSE ALARMS

There are four basic reasons for false alarms, and the secret to reducing them is to clearly identify the cause and make proactive corrections:

1. Lack of proper education on how to enter and exit the facility, such as improper arming and disarming of the intrusion detection system using a keypad.
2. Weather-related issues.
3. Equipment failure (dead batteries) or poor installation.
4. User error (forgetful or unknowledgeable uses).

Approximately 95% of all alarm activations are false and must be addressed proactively to prevent security/protection officers and employees from becoming complacent or failing to respond to alarms.

55. SECURITY/PROTECTION OFFICER INSPECTION CHECKLIST

Close supervision is required for the protection/security officers and random, unannounced inspections should be conducted periodically. All posts and patrols should be monitored and evaluated for their effectiveness. The following checklist has been developed to assist you in performing this inspection quickly and efficiently.

SECURITY/PROTECTION OFFICER'S POST ORDERS/SECURITY MANUAL INSPECTION

1. Are the post orders or security manual current? When was the last revision date?
2. Is each officer's post equipped with current post orders or a security manual?
3. Has each officer been properly instructed on the post orders and the use of the security manual?
4. Do the security manual and post orders contain the following information?
   a. General duties
   b. Instructions and duties for all posts
   c. Duties of security supervisors
   d. Procedures: doors, windows, building checks
   e. Procedures to deliver reports
   f. Vehicle and gate procedures
   g. Package/equipment pass procedures
   h. Control procedures for inbound and outbound company vehicles
   i. Control procedures for inbound and outbound vendor vehicles
   j. Control procedures for inbound and outbound vehicles
   k. Employee and visitor parking procedures
   l. Personnel gate control procedure
   m. General access control procedures
   n. Procedures for handling visits by union representatives
   o. Procedure for handling visits by government inspectors
   p. Instructions for handling natural and man-made disasters and emergency situations
   q. Emergency telephone numbers for police, fire, ambulance, etc.
   r. Emergency contact list for site
   s. Supervision emergency contact information
   t. Identification badge systems for employees and nonemployees
   u. Instructions for proper recording and control of all pertinent information: gate logs, telephone logs, etc.

SECURITY/PROTECTION OFFICER'S POST INSPECTION

1. Is the officer in the required uniform?
2. Does the officer take pride in the care of his or her uniform and personal hygiene?
3. What is the officer's attitude? Positive and upbeat?
4. Does the officer perform his or her duties efficiently as prescribed in the security manual or post orders?
5. Has the officer been properly trained so that he or she is not only knowledgeable about the duties of his or her own post, but also cross-trained on other posts at the site?
6. Is the officer aware of his or her authority and the limitations of that authority?

7. Is the officer alert to his or her surroundings—situationally aware and not complacent?
8. Is the officer disciplined, but courteous and tactful in the performance of his or her duties dealing with the public?
9. Is the officer clean and orderly and always in assigned uniform?
10. Are all required documentation current and accurate?
11. How does the officer feel about his or her duties and responsibilities?
12. Does the officer have any recommendations about increasing the efficiency of the present security post?

SECURITY/PROTECTION OFFICER SUPERVISOR'S INSPECTION

1. Is the supervisor in the proper uniform?
2. Does the supervisor take pride in the care of his/her uniform and personal hygiene?
3. Is the supervisor properly training all of the security officers?
4. Does he or she update the officers in procedural changes, etc.
5. Does he or she maintain accurate records on officers' performance?
6. Does he or she maintain effective control of all required documentation?
7. Does he or she maintain control of officers so that maximum efficiency, discipline, and morale are obtained from each?
8. Does he or she accurately report to his or her manager so that management is current on all pertinent information?
9. Does he or she handle and document complaints and violations in accordance with the procedures outlined in the security manual/post orders or company policy?
10. Are monthly inspections conducted of all in-house equipment documenting needed repairs and/or replacement?

56. TRAINING FOR SECURITY/PROTECTION OFFICERS: DO NOT TAKE TRAINING LIGHTLY

Over the years, we have all received training that has helped us get to where we are today. But as the one conducting the training, its a different situation—it takes time and effort to put together a quality presentation. It is often said that for every 1 h of presentation time, 4 h must be spent preparing. We learn valuable training techniques from professional training programs, instructors in university and professional development classes, and also from mentors. One instructor that we remember came bursting into the classroom at exactly the time class was to start, with the door swinging wide open and banging into the wall. Students would jump and heads would turn. Tim Crowe at National Crime Prevention Institute would walk up and down between the tables and chairs in the classroom. Some

trainers or instructors stand at a podium, some pace in front of the room, and others walk around the classroom. The point is, everyone who teaches, develops a style to effectively relay information.

Marianna Perry's style is to create PowerPoint slides to ensure that she stays on the topic and then hand out a copy of her presentation so that class participants will receive all of the information on the subject. She talks about projects that she has been a part of where the material she is presenting proved to be successful.

Larry Fennelly's style is a combination theory and practice. If he is talking about the Crime Displacement Theory, he will tell you about it and then give examples of how he was successful moving crime and reducing criminal opportunity. Our point is everyone develops a presentation style.

WHY DO WE TRAIN?

Over the years, employees have been trained so that they will be able to do a better job and also understand what they are expected to do and how they are expected to do it. Lesson plans should be the same way—clear and updated, with the very latest information available. How do you expect a security/protection officer to respond to an alarm system if you do not teach him or her how the system works? Today, we live in a world of passwords for virtually every device and every system. This is critical information. When an alarm goes off at 3:00 a.m. and the siren is blasting, and no one knows the password to reset the system, it is a problem. The next morning, you may have to explain to management why the alarm system is damaged because no one knew the password to reset the system. We must adequately train security/protection officers to effectively do their jobs. If you want to reap the rewards of being efficient and professional, you properly train and then document the training. Training should not be taken lightly. It is too important to leave job performance to chance.

TRAINING FOR SECURITY/PROTECTION OFFICERS

At a minimum, security/protection officers should be trained and tested on the following topics:

- Post orders
- Basic security officer responsibilities
- Ethics and professionalism
- Personal appearance
- Human relations, customer service, public relations
- Personal safety
- Situational awareness
- Communication policies and procedures
- Telephone and radio etiquette
- Security policies and procedures
- Access control (personnel and vehicles)
- Patrol procedures
- Observation techniques

- Challenging techniques
- Crowd control
- Blood-borne pathogens, first aid, and CPR/AED Training
- Ingress and egress control
- Operation of security systems (IDS and video surveillance)
- Safe driving (if mobile patrol)
- Criminal and civil law
- Investigations
- Legal authority and scope of responsibility
- Use of force
- Relations with law enforcement
- Conducting investigations
- Evidence preservation
- Report writing
- Responding to emergencies
- Terrorism threat awareness and weapons of mass destruction
- Workplace violence
- Active shooter/active assailant
- General fire prevention and safety and fire drills protocols
- Hands-on fire extinguisher usage
- Bomb threat procedures and Emergency Management Procedures

57. THE ART OF TRAINING

Training the trainers is not a new idea; it has been around for years. Making it work, requires training, material, and the knowledge of "How to Teach." Teaching, lecturing, and giving a talk all require a different approach.

Teaching requires that you exert influence on the minds of the students and take them into areas that they have never been before; it is also selling them on a product that they will remember.

Teaching is said to be based on three great principles:

1. I hear—I forget
2. I see—I remember
3. I do–I never forget

VISUAL AIDS

Visual Aids are important when training. Consider using some of the following visual aids:

- Overlays (rarely used)
- Blackboard
- Flip charts
- Overhead projector for PowerPoint

- Slide projector (rarely used)
- VCR—video camera
- Go-Pro camera and playback display

There are two golden rules for using visual aids:

1. Do not have too many visual aids.
2. They must be well presented, professionally prepared and presented.

Rules for use of any equipment:

1. Test it before class and ensure it is working.
2. Check slides, make sure none are upside down.
3. Use multicolored chalk or pens (except for the color red in a PowerPoint).
4. Use a laser pointer; do not walk in front of a picture; talk to the side.
5. Check microphone, podium, and your notes.

INTRODUCTION

Each person who is to give a presentation should be introduced as if he or she is someone special. Their qualifications, read expertise, should be identified and the subject matter should be stated. Emphasize their expertise.

LECTURING VERSUS TEACHING

Lecturing usually requires you to talk for a fixed period of time. Preparation to give a lecture usually takes twice as much time as the actual lecture is going to take. Rehearse your presentation and time it. If you have an hour-long presentation, tell the class you will be allowing 10–15 min for questions and answers at the end of the lecture. Consider the use of case studies and new technologies like Prezi.

CONTROLLING THE CLASS

1. Controlling the class starts when you start the program on time, for example, 8:00 a.m. versus 8:20 a.m. If the class starts 20 min late because two students are late, the students control the class and not the instructor.
2. Request that the class take notes (supply pencil/pen and paper). Emphasize the key points during the class.
3. Encourage an exchange of questions. You can ask the questions, but you know the answer and the person you are asking. Do not ask difficult questions because they may turn off the class.

If you are asked a question, and do not know the answer, do not fake it. Admit you do not know the answer, and ask if anyone in the class knows the answer.

Here are some tricks of the trade in answering questions:

- "Will you ask that again? I don't think everyone in the class heard you?" Having a question repeated does two things: it gives you time to collect your thoughts, and the second time around, the question may be worded differently and to your advantage.
- Praise the student who asked the question. It is like a pat on the head. "This was a very good question; I hope I answered it properly."
- Do not fake an answer that you do not know.
- Phrases like that can save you: "Correct me if I'm wrong…" "In my opinion…" (and answer the question).

HANDOUTS

Everyone has handouts, and management expects it. Handouts should relate to the subjects being discussed. As a general rule, handouts should be distributed after the presentation because they will be a distraction. Review the handout material very carefully.

PLANNING

Teaching and lecturing require not just a degree of knowledge on a specific subject but also require you to know your audience.

Sessions should be planned, for example, a 50-min program and 10-min breaks. One 20-min break in the morning and afternoon can be provided. Lunch time should to be decided. Your program must fit around the above or similar time frames.

If your program is planned and advertised 9:00 a.m. to 5:00 p.m., you should start at 9:00 a.m. sharp and finish at 4:50 p.m. to 5:00 p.m.

VOICE CONTROL

In "My Fair Lady," (1964) Eliza Doolittle was transformed from a Cockney flower girl to a lady of gentility. Her voice quality and her diction were the focal points of the movie. Remember to speak clearly and raise and lower your voice as you speak. Do not forget to also make eye contact.

Below are some helpful hints:

- Speak as if you are speaking to this end of the room.
- Look at the person you are speaking to.
- Pay attention to questions being asked.
- Never interrupt.
- Use the proper volume in voice control.

NERVOUSNESS

Depending upon the type of program and the experience of the presenter, nervousness comes in degrees. If you are drinking coffee or water, the class should be allowed

to. Everyone is nervous in the beginning of a presentation until they get started. Consider doing the 7:00 p.m. news on CNN and you must wait in a chair, under strong lights, at 6:30 p.m. until 7:00 p.m. Your presentation is easier.

RECORDING DEVICES

I have read for a specific seminar recently the following: "Recording devices will not be allowed." The subject matter and the reason why the person wants to record the session will aid in your decision whether or not to allow recordings of sessions.

ENDING YOUR PRESENTATION

In every book or story there is a golden rule: strong beginning and strong ending. This rule will make you become creative and force you to provide a strong finish.

58. SECURITY/PROTECTION OFFICERS AND PROFESSIONALISM

The growth in the private security industry has increased the need for competent, security professionals. Some professional acceptance can be achieved through educational programs and professional development, but what does it really mean to be a "professional"? Most of us have probably not been formally taught about professionalism and are instead supposed to learn it on our own, but that is sometimes a difficult way to learn things. Being a security professional means displaying competence in your area of expertise *and* knowing your strengths and weaknesses. Strive to demonstrate the core values of competence and professionalism. For example, wear the appropriate business attire and practice proper workplace etiquette. Whenever possible, take on leadership roles and show that you are willing to accept result-driven responsibilities.[50]

59. THE IMPORTANCE OF PROFESSIONAL CERTIFICATIONS: ASIS INTERNATIONAL AND THE INTERNATIONAL FOUNDATION FOR PROTECTION OFFICERS

Professional credentials may be the single determining factor for advancement in the security profession. Education may be from a degree granting, academic institution or a professional association, such as ASIS or International Foundation for Protection Officers. Gaining knowledge in an academic program may come in the form of certification or accreditation. The credential must be based on something gained and high standards of program credentialing that are recognized by the professional associations that represent the field and discipline.[51]

[50] Davies SJ. *Women in the security profession: a practical guide for career development*. Elsevier, Cambridge, MA; 2017.
[51] http://ipca-cert.org.

ASIS International was the first organization to implement security certifications and develop a standard for excellence in the security industry. The following ASIS security credentials are accepted throughout the world and are proof of professional knowledge:

- Certified Protection Professional *Board Certification in Security Management*
- Professional Certified Investigator *Board Certification in Investigations*
- Physical Security Professional *Board Certification in Physical Security*[52]

The International Federation for Protection Officers offers the following educational and certification programs for security professionals:

- Certified Protection Officer Program
- Certified in Security Supervision and Management
- Certified Protection Officer Instructor[53]

60. GUARD HOUSES/GUARD BOOTHS

The presence of a security officer in a guard house/guard booth is not only a visual deterrent but also a security component that can control vehicle and/or pedestrian access to an area or a facility, monitor video surveillance, check credentials, and restrict access, when necessary.

Guard houses/guard booths are available in different sizes—both prefab and built on-site, designed by architects, or assembled from a crate—depending on the security application. Some are very elaborate with modern technology and many conveniences, whereas others are very small, simple buildings intended to protect the security officer from the elements when performing his or her duties (see section on lighting and for more information on guard houses/guard booths as well).

It is important to have a trained professional and competent security officer in a guard house/guard booth because of their constant interaction with the public. They must be observant for suspicious activity and be able to quickly determine if a vehicle or person is dangerous.

61. PHYSICAL SECURITY EXPENSES AND MAINTENANCE

Physical security is the use of numerous and diverse devices, hardware, technology, and other various types of equipment to control access, secure property, and detect intrusion or environmental concerns. The types of hardware and technology in use today include, but are not limited to, the following:

- Electronic locking devices
- Video surveillance systems (CCTV)

[52] www.asisonline.org.
[53] http://www.ifpo.org.

- IP cameras, with video analytics
- Monitoring equipment
- Digital recording equipment
- Intrusion, panic, and barrier alarms
- Fire detection and suppression equipment
- Mirrors (especially in a retail environment)
- Cost-effective and energy-efficient lighting
- Emergency lighting
- Redundant communication systems and notification devices
- Access control devices, such as smart cards
- Biometrics for access control
- CPTED-compliant design of the perimeter of the property and buildings

Ensure that service and maintenance is included for all security components and that you have budgeted for system upgrades, when necessary.

Furthermore, there are varieties of fencing, walls, and other barriers designed to protect the property, its contents, and its occupants. Although security departments have varying degrees of involvement in the selection and installation of equipment, they all use it and are frequently responsible for monitoring and maintaining it.

The various security equipment and systems available to us are very useful in augmenting the efforts of the security staff. However, security managers should be cautious not to depend solely on hardware. Effective and consistent human security practices are the key to the success of the security program. In addition, security managers should have contingency plans in case a piece of hardware fails, someone tampers with it, or there is a temporary loss of power. As our society becomes more technologically oriented, the risk of becoming too dependent on electronic security equipment increases. In all environments, adequate security still requires a well-trained, alert, and conscientious security staff and the integration of basic security concepts into all aspects of the operation.

62. BUDGETS: LEASING VERSUS PURCHASE

If leasing equipment in support of your security processes, it is recommended that you do so with the option to purchase. Short-term or long-term leases should allow for a buyout. Be mindful of negotiating repair, maintenance, and extended warranty provisions into the language of your lease. It is also possible to negotiate a discount for parts, repairs, and supplies.

The practice of "renting" or short-term leases for equipment to be used in support of an on–off operation or an investigation many times extends to longer periods of time than originally anticipated. The option to purchase after 90–120 days frequently covers the cost of the equipment.

The practice of negotiating deep or progressive discounts should not be overlooked. The possibilities of vendor competition, overstocked inventory, sales pressure, and poor field office performance all combine to put pressure on sales and installation vendors.

It would be difficult to consider physical security without accepting the issues and necessity for capital investments. This obviously requires budget preparation. Many security managers adopt a position that the security function contains too many variables and is subject to unforeseeable events that are peculiar to the discipline and render budgeting difficult, if not impossible. They operate with a variety of believed perceptions that include "the squeaky wheel gets the grease" (that is, if you scream the loudest, you will get the support); just add 15% to last year's budget; or "Submit what we asked for last year, but add 10 percent across the board." This budget philosophy is unprofessional and irresponsible. We suggest that there are three basic areas that must be included: fixed, controllable, and unforeseen expenses. Based on past experience, we would suggest that a rule of thumb for arriving at unforeseen contingency expenses is to base it upon 40% of the combined total of fixed and controllable expenses. And, contrary to some practices, any unapplied funds from the unseen contingency funds are returned to the general operation surplus fund.

63. BUDGETING: ART OR SCIENCE?

A simple definition of "budget" is an attempt to place in document form, the costs of operating security services for a period of time. The document form may be a narrative, computerized spreadsheet, ledger, or justification memorandums. This combination of numbers and words refers to the fixed, controllable, and unforeseen expenses. The period of time for a budget is usually 1 year, and various companies determine specifically what their fiscal year shall be. The complex task of budgeting for unforeseen security expenses is difficult, if not impossible. Such events as natural disasters, labor disruption/strikes, damages to the business due to fire or sabotage, major theft, or fraud investigations are but a few of the unforeseen services that the security function may be called upon to provide.

The fixed operating costs associated with security staffing of either proprietary or contract services is predictable. Included are such obvious items as salary, benefits, training, and uniforms, if they are required. The use of facilities and related support or general expenses might be allocated to the security department on a prorated basis. If this practice is followed in an organization, it should also dictate that the cost of security services be allocated back to the various departments that benefit from security support services. Frequently, security is called upon to provide ancillary support duties and functions to operating departments.

There is the belief among many security managers and directors that security budgets are extremely difficult to control. Yes they are difficult, but not impossible. The services that security provides are measurable, and the effectiveness of the services that are provided are reasonable. The quantity and the quality of the services performed are measurable. The standards which measures can be drawn from are currently known as "Best Practices." Controlling security costs begins with the effective use of security staff and an understanding of vulnerabilities as well as policies and procedures. An ineffective, inexperienced security manager may expend

$200,000 to correct a $15,000 problem or concern. Frequently, effective use of the security staff and adjustments in simple procedures can eliminate problems without increased costs.

It is our opinion that the purpose of the security function in the business environment is to enhance profitability through controls and prevention techniques—basically a system of checks and balances. Such prevention efforts are directed at losses caused by theft, fraud, damage, natural disasters, and internal and external threats of all types. It is impossible to rationally address the fabric of security without including the varied, and at times, complex needs necessary to accomplish tasks without the benefit of financial resources. Therefore, what is required is a detailed short- and long-term plan to guide security needs. Simply put, you must have a security budget.

Budgets or a financial needs plan are formalized and sophisticated in large companies and organizations. Frequently, they are submitted on electronic spreadsheets, which senior management may require from all operations and departments within the organization. Financial security needs are not only a "big" company requirement but also apply to small and even one-person security departments.

64. DATA CENTER AND SERVER SECURITY

Data center and server security is a critical operation for any organization because of the need for effective storage of confidential and valuable information. A data breach can be devastating to organizations, regardless of their size. Business partners and customers may lose their confidence that the organization can keep confidential information confidential, and this in turn may result in financial losses.

When determining the level of security for a new or existing data center or server room, a risk assessment must be conducted to assess both the data stored and the equipment in the facility using an impact versus likelihood approach. The assessment will be the basis for adequate security to potential threats. Part of the process for a data center or server security process also involves quickly identifying a breach and then containing it as soon as possible.

The following are industry standards and legal requirements for organizations that safeguard sensitive or confidential data:[54]

SSAE 16: Statement on Standards for Attestation Engagements (SSAE) No. 16 replaces the previous Statement on Auditing Standards (SAS) No. 70. The SSAE 16 is widely recognized as an auditing standard developed by the American Institute of Certified Public Accountants. Adequate controls and safeguards are required for host or process data belonging to customers. These controls may include physical security requirements such as two levels of authentication for electronic access, "man traps" on the data center floor, and a process for individuals requesting access.

Section 404 of the Sarbanes-Oxley Act of 2002 makes SSAE 16 more important for reporting the effectiveness of internal controls over financial reporting.

[54] https://www.anixter.com/content/dam/Anixter/White%20Papers/12F0010X00-Four-Layers-Data-Center-Security-WP-EN-US.pdf.

Introduction Industry Standards and Legal Requirements Technological and Internal Challenges 4 ANSI/TIA-942: this standard is recognized throughout the industry for data center infrastructure requirements to provide information to planners regarding the protection of data center/server assets by utilizing physical security as well as fire prevention. It recognizes the importance of providing manageable access control to data center facilities and monitoring of people and their actions. Using the Uptime Institute Tier framework as a basis, the *ANSI/TIA-942 Standard* makes recommendations on the facilities specifications and improving the physical security of the data/server center. These include criteria such as video surveillance recording frame rates, access control levels, and hardware and site selection. There are recommended specifications by tier as a uniform way to rate aspects of a data center design utilizing qualified architects and engineers.

The Health Information Security Rule Safeguard Standards and Payment Card Industry Data Security Standard mandate that certain access restrictions be in place for data/server center facilities and also require the reporting and auditing of access be provided. There are also directives from the Department of Homeland Security if the data are deemed vital to national and economic security.

The following are some basic principles for data center and server security:[55]

- Do not identify the building as the "Data Center" or the room as the "Server room." Identify by number and/or address only.
- There should be four sources for utilities—electricity, water, voice, and data. Trace electricity sources back to two separate substations and water back to two main lines. The lines should be underground and come into different areas of the building. Utilize the anticipated power usage as leverage for accommodating the building's special needs.
- Use concrete walls to secure generators located outside the building.
- The walls should be constructed of 1-ft-thick concrete to be effective barriers against the elements and explosive devices.
- Avoid windows completely or only have them in the break room or administrative area and ensure that they are double glazed or shatter resistant.
- Control access to the parking lot with permanent security officers and a guard house. The gated entry can be opened remotely or through the use of retractable bollards. A winding entry route will limit the speed of vehicles approaching the facility.
- To protect from vehicles, install bollards or planters around the perimeter of the building.
- Limit access points to the building—one main entrance in front and a rear entrance with a loading dock in the rear.
- Utilize anti–pass-back and mantraps. Tailgating (following someone through a door before it closes) is one of the ways that an unauthorized visitor can gain access into a data center. By implementing mantraps that only allow one person through at a time; you force visitors to be identified before allowing access.

[55] http://www.datacenterjournal.com/a-guide-to-physical-security-for-data-centers/.

- Fire doors should be exit only and equipped with intrusion detection, a propped door alarm, forced door alarm, as well as open/close alarms.
- The perimeter of the building and the entry/exit points should be monitored by video surveillance. Access points throughout the building interior should also be monitored.
- All contractors, vendors, and repair personnel should be escorted and accompanied at all times while on the property.
- Ensure that the HVAC system has the capability to recirculate air rather than drawing it in from the outside, if necessary. This will protect building occupants and equipment should a biological, chemical, or radiological agent be introduced. You may also want to consider monitoring the air in the building.
- In the secure areas of the data center, ensure that the walls run from the slab ceiling to the subflooring where wiring is typically housed. Ensure that drop-down ceilings do not provide hidden access points.
- Use two-factor authentication. Biometrics is becoming the standard for access to sensitive areas of data centers. Hand geometry or fingerprint scanners are considered less invasive than retinal scanners.
- Ensure you are utilizing layered security. For example, at the front door, use a card reader and entry code panel. At the inner door, ensure that the visitor area is separated from the general employee area. At the "data" location, use strict controls, such as a floor-to-ceiling turnstile to prevent piggybacking or a "man-trap" consisting of two separate doors with an airlock in between so only one door can be opened at a time.
- At the door to the computer processing room where servers or mainframes are located is usually the layer that has the strongest "positive controls." Control and track access.
- At the door to an individual server cabinet, racks should have lockable front and rear doors that use a three-digit combination lock as a minimum. This is a final check, once someone has access to the data floor, to ensure they only access authorized equipment.
- Do not allow food or drinks in the computer rooms, so ensure there is a common break area.
- Install visitor rest rooms so that visitors, contractors, or repair persons do not have access to the secure areas in the building.

65. LOADING DOCK AND CHEMICAL STORAGE SECURITY

LOADING DOCKS

1. Control access to the area. It is recommended that the gate or overhead doors to the loading dock be kept shut at all times. Vehicles should be allowed to proceed only after being confirmed and inspected by security.
2. Inspect delivery vehicles. A protocol consisting of a quick visual or technological inspection utilizing trace detection machines must be conducted prior to vehicles entering the loading dock.

3. Create a stationary security post. A security officer must be assigned to the loading dock to not only inspect incoming deliveries but also monitor for unauthorized access (particularly since the loading dock allows for direct entrance to the facility). This post needs to be equipped with a video surveillance monitoring station to observe for incoming delivery vehicles.
4. Hazardous material storage, such as toxic industrial chemicals (ammonia, chlorine, and hydrogen cyanide and potentially more unknown chemicals) may be in the loading dock area, particularly if the facility is an educational or research center with laboratories.
5. The valve protection caps shall be in place and secured on all gas cylinders. Unless cylinders are firmly secured on a special carrier intended for this purpose, regulators shall be removed and valve protection caps shall be put in place before cylinders are moved. A suitable cylinder truck, chain, or other steadying device shall be used to keep cylinders from being knocked over while in use. Compressed gas cylinders shall be secured in an upright position at all times except, if necessary, for short periods of time while cylinders are actually being hoisted or carried. Inside of buildings, cylinders shall be stored in a well-protected, well-ventilated, dry location, at least 20 ft (6.1 m) from highly combustible materials such as oil or excelsior. Cylinders should be stored in defined, assigned places away from elevators, stairs, or gangways. Assigned storage places shall be located where cylinders will not be knocked over or damaged by passing or falling objects, or subject to tampering by unauthorized persons. Cylinders shall not be kept in unventilated enclosures such as lockers and cupboards.
6. NFPA 1600 is needed for all hazards planning.
7. Provide Federal Emergency Management Agency training for administration and crisis team members.[56]
8. In an emergency:
   a. Develop a preplan for your facility with key elements. Preparedness can fall into the operational and/or procedural guidelines.
   b. Understand response agency actions at *your* facility during a crisis response, not during normal day-to-day operations.
   c. Develop the Facility Liaison Officer to fully integrate/coordinate with the response agency officials to mitigate the impacts of the event.

CHEMICAL STORAGE

Access Control

The doors from corridors leading to the chemical storage area must be secured and kept shut at all times. Chemical storage rooms must be put on a separate key group, making it a secure area.

Card readers need to be installed on the doors leading to the chemicals storage rooms, giving access only to security and authorized personnel.

[56] http://training.fema.gov.

Video Surveillance

Every access point to chemical storage areas should be monitored by video surveillance. An additional camera may need to be installed inside the chemical storage room.

Cabinets

Individual cabinets where hazardous materials are stored need to be secured at all times. We recommend using padlocks that have an American Society of Testing Materials certification and have no markings that will identify the key to a specific location.

66. THE SIX MOST CRITICAL AREAS IN A STORAGE FACILITY

Every facility requires a careful analysis of the most vulnerable areas of attack, most easily identified during a security assessment. The six most critical areas in a storage facility are usually centered in, but not limited to:

1. Overhead doors that are used for deliveries and shipping
2. Exit doors and fire doors (emergency exits)
3. Outside perimeter walls
4. Interior doors that are on access control
5. Ceiling or cabling/utility areas
6. Interior storage areas

Each of these areas must be protected regardless of the number of security officers on the premises. Although conventional alarm devices are available to protect vulnerable areas, certain modifications can be made to improve the system to meet specific needs.

Because cargo facilities are resorting to larger storage containers, the obvious movement of material in and out of the facility will often involve large overhead doors. It is estimated that 70–80% of all undetected theft leaves facilities through overhead doors, during normal working hours, unless they are protected.

67. PARKING FACILITY SECURITY[57]

Issues:

- There are hiding places between parked cars.
- Parked cars affect the distribution of light.

[57] Fennelly LJ. *Handbook of loss prevention and crime prevention*, 5th ed. Elsevier, Boston, MA; 2012.

- Most parking facilities are open to the public.
- An offender's car may not be memorable.
- Parking garages are preferred over parking lots because land is valuable.

Since parking facilities usually encompass a large area with relatively low levels of activity, violent crime is more likely to occur, but CPTED principles may help reduce the fear and risk of crime. Natural surveillance may work for low-risk facilities, but higher risk areas may require access control. Access control and perimeter security are best considered when the parking structure is being designed.

Security screening or fencing can be provided at points of low activity to keep someone on foot out, but will still allow the structure to seem open. Ground-level pedestrian exits that open into nonsecure areas should be emergency exits only and filled with panic bars. A local alarm should activate if the door is opened.

Attendant booths and security offices should be located where they can monitor activity in the facility—preferably at entry and exit points. If a driver is required to take a ticket on entry and is observed by video surveillance and then also has to interact with an attendant or security officer when he or she exits, the facility will be less attractive to criminals than one that is open and unattended—think about crime opportunity.

Pedestrian paths should be planned to concentrate egress from the facility. If all pedestrians are brought through a central port, rather than allowing them access through several routes, it improves the likelihood that they will see and be seen by other people in the parking facility.

Placement of signs and graphics help orient parking facility patrons and allows them to move quickly in and out of the facility and make them less vulnerable to an attack.

Color coding parking garage levels will help patrons quickly recall what level they parked on.

Public restrooms in parking facilities present a security issue because of infrequent use and because they are hiding places. If restrooms do exist in a parking facility, they should have a maze-type entrance instead of inner doors and be visible to the attendant booth or the security office.

Shrubbery should be planted away from the facility and trimmed to eliminate hiding places. If there are visible cameras, signage that the area is being monitored by security officers—criminal activity may be deterred.

Passive security: physical features that incorporate CPTED principles.

Active security: human activities such as security officers on patrol, intercoms, duress buttons, emergency phones, and sound surveillance and monitored video surveillance.

CPTED should be a high priority in all parking facilities because:[58]

- Natural surveillance is a low-cost crime prevention strategy.
- Even if security is not an issue at a specific location today, it may be in the future.

[58] National Institute of Justice, Crime Prevention Through Environmental Design in Parking Facilities, 1996.

- Active security will lessen the likelihood that a crime will occur and reduce the liability of the parking facility owner if it does.

Lighting is a key component in the security system in a parking facility, so lights must be reliable, easy to maintain, be able to withstand the elements, and also be protected from vandalism.

HOW TO IMPROVE LIGHTING BRIGHTNESS IN PARKING GARAGES

Staining concrete is a cost-effective way to increase brightness and to create a sense of well-being. White stain on ceiling and beam soffits reflects light and increases uniformity. Concrete stain will last about 10 years. Paint achieves the same increased level of brightness, but requires more maintenance. White stain or paint increases the likelihood of graffiti, which decreases the perception of security. Antigraffiti coatings may be used on walls so that graffiti can easily be removed and the walls cleaned. There are two categories of concrete stains, reactive and nonreactive.

Reactive stains are water-based acidic solutions containing metallic salts that react with the concrete's lime content. Once the chemical reaction takes place, the stain forms a permanent bond with the concrete and will not chip off or peel away.

Nonreactive stains are water-based acrylic stains that do not rely on a chemical reaction to impart color. Instead, they are formulated to penetrate the concrete surface and deposit their pigment particles in the open pores. Nonreactive stains are water based and more commonly used, come in more colors, and are easy to apply.[59]

68. EMERGENCY (BLUE LIGHT) PHONES/CALL STATIONS

Emergency (blue light) phones or call stations are ideal security solutions for remote and/or high-risk areas. Emergency phones and call stations can offer immediate assistance and a quick response by security personnel. Additionally, most models include video surveillance capabilities and a blue light that is always illuminated, mounted on top of the unit to give high visibility and a feeling of security to people in the area. Patrons can call emergency personnel with a simple push of a button. At this same time, the blue light on top of the unit will begin to flash, attracting attention to the location. The face plate on blue light emergency phones is illuminated at all times for clear visibility at night. Emergency blue light phones are vandalism resistant and designed to operate in extreme weather situations.

Emergency blue light phones are commonly used on university and college campuses, parking facilities, shopping malls, medical centers, industrial campuses, and many transit facilities.

[59] https://www.pci.org/WorkArea/DownloadAsset.

69. BUILDING SITE SECURITY AND CONTRACTORS

It is safe to say that most contractors will experience some theft of tools, building materials, or supplies before completion of a long-term construction project. They should be made aware of this fact and be security conscious at the beginning of the construction project before thefts get too costly. Thefts that appear to be of an internal nature should be analyzed against such thefts at other sites, and security measures put into place.

The following is a checklist for contractors:

1. The contractor should appoint security/protection officers or a liaison staff person to work with law enforcement on matters of theft and vandalism.
2. Perimeter protection:
   a. Gate type and strength
   b. Hinges
   c. Locks and chains
   d. Lighting
   e. Know the crime rate and offense types in the neighborhood
   f. Install a 6–8 ft (depending on the application) chain-link fence with three rows of barbed wire or razor wire.
3. Location of contractor's building on-site:
   a. Inspect the security components of the building
   b. Review site security procedures and controls
   c. Light the building inside and out.
4. Materials and equipment on-site should be protected in a secured yard area.
5. Facilities for storage and security of tools and clothing should be kept locked and in a secure area.
6. All subcontractors are responsible to the main contractor.
7. Security/protection officers should patrol at night and on weekends.
8. Use temporary alarm protection for the site.
9. Payment of wages to employees should be made with checks, not cash.
10. Deliveries of valuable material to site should be secure and such items should be stored in a secure area.
11. Establish a method to check accurate deliveries by using authorized receiving persons.
12. Check for proper signage around the perimeter of the building and the property.
13. Identify easily transportable material and property and be knowledgeable about common construction site thefts.
14. Have procedures in place to report theft:
    a. Local law enforcement
    b. On-site security officers
    c. Office and insurance company

Have a security officer on duty at the construction site? We heard the story once of a construction site that was experiencing a large number of thefts—both supplies and tools. The contractor contacted several contract security companies, but only one had experience in construction site security and also gave a proposal that was acceptable. The company was awarded the contract and thefts at the site were stopped. At 3:30 p.m. the Security/Protection Officer showed up, ready for duty. He was 6 ft 5 in. tall, 240 lbs., and all muscle. He carried a Glock 40 on his right hip, a shot gun, and two belts of shells over his shoulders. He basically looked like a Mexican bandito from an old cowboy movie. Also, he had two German shepherds that patrolled the interior of the building and the perimeter of the property. Within several days, he fired his shotgun four times up into the air. That was it. There were no more crime problems. The protection exceeded the norm but worked to reduce losses. We are certainly not endorsing this approach, but this is an example of reactive, excessive security.

70. INADEQUATE SECURITY AND SECURITY LIABILITY[60]

Inadequate security is generally referred to as *premises security liability*, that is, the civil liability of owners for the foreseeable criminal acts committed by third persons. Inadequate security claims arise when a property owner fails to provide a reasonably safe environment, and as a result, someone is victimized by the criminal conduct of another person.

The owner of the property may be held liable for a crime if there has been a pattern of crime on or around the property, or in other words, if there was *foreseeability* that a crime may occur on the premises.

The property owner may be found by a court to have a legal duty to implement reasonable security measures such as the following which are designed to prevent or deter crimes:

- Perimeter protection
- Adequate lighting
- Security officers
- High-quality locks
- Video surveillance system
- Badge and/or key control
- Alarm systems (intrusion and fire)
- Controlled access to parking areas

If the property owner is found by the court to have known about previous crimes on the property, but did not provide adequate security, the owner may be found liable for injuries or death on the property.

[60] www.asisonline.org/poa.

LIABILITY AND PHYSICAL SECURITY

The first question will be, "Did the company have a duty to take action and to protect their assets?" (meaning their employees).

If we assume that after notice was given to you of an incident and you did nothing, you failed in your duty to take corrective action, it means you failed to provide a reasonable degree of care as it pertains to the incident.

Liability in the early stages is not complicated—simply practice due diligence by providing a reasonable level of security. Key steps are:

1. Have a physical security/risk assessment conducted to identify your vulnerabilities.
2. Take steps to address the identified vulnerabilities.
3. Implement security measures that are considered "Best Practices" in the security industry.
4. Establish security policies and procedures and ensure compliance through regular audits.
5. Have a qualified instructor train your employees.
6. Document training.

Now let us assume your facility has done none of the these steps above and you have an employee attacked, a personal vehicle or personal property stolen, etc. Now, ask yourself the following questions:

1. Did you have a duty to protect your employee and their property?
2. Did you provide a reasonable degree of care? (This is why you must have documentation to show what action you took as well as the specific steps).
3. Did you provide reasonable security to keep your employees safe?

Your failure to do so may be the proximate cause of the incident. Now the question is, "Was the crime a foreseeable act?"

Over the years, we both have done numerous physical security/risk assessments and have asked facilities managers the following question or something very similar, "I noticed your lights were out in the back parking lot" and the reply is, "Oh, they've been out for 2 years now because somehow the wires got cut."

We were recently conducting an assessment for a facility that had over 1500 active badges but we only had 990 employees. This was a red flag for issues.

During assessments, we have both asked managers, "How many cameras do you have on the property?" Many times there was a smile before they replied, "Only 2 dummy cameras." "Dummy" cameras are many times placed by dumpsters in an attempt to deter theft or in remote areas on the property. We have seen poor maintenance of physical security components and no room in the budget for replacement equipment, so many times the same issues continue for years.

PART

Assessing Risk and Vulnerabilities

2

71. THE FOUR D'S: DETER, DETECT, DELAY, AND DENY

Crime prevention has four D's when it comes to opportunity:

- *Deter* criminal attack
- *Detect* attacks that occur
- *Delay* attack to allow time for authorities to respond
- *Deny* access to selected targets

72. WHAT IS A SOFT TARGET?

The Oxford Dictionary defines soft target as "a person or thing that is relatively unprotected or vulnerable, especially to military or terrorist attack."[1]

In her book, *Soft Target Hardening*, Dr. Jennifer Hesterman defines soft targets as civilian-centric places that are not typically fortified. They are vulnerable, unprotected, and undefended privately owned property. They may possibly be resource constrained, and security may not be a primary mission of the organization. Soft targets may be colocated or near a hard target.[2]

Soft targets can be identified as churches and other houses of worship; schools, colleges and universities; hospitals and health care facilities; shopping malls and strip malls; sporting and recreational venues; concerts, hotels, motels, and resorts; office buildings; as well as critical infrastructure systems. Basically, a soft target is any person or thing that is vulnerable to attack, but is not protected. This could be virtually any location in any environment without sufficient security measures in place to protect their assets. It could also be people who are not capable of protecting themselves from attack or people who are unaware that they are vulnerable because of an existing threat. A Threat Risk Assessment (TRA) will help identify vulnerabilities.

[1] www.oxforddictionaries.com/us/definition/american_english/soft-target.
[2] Hesterman JL. *Soft target hardening: protecting people from attack*. CRC Press, Florida; 2014.

Physical Security: 150 Things You Should Know. http://dx.doi.org/10.1016/B978-0-12-809487-7.00002-4

73. THREAT RISK ASSESSMENTS

As you start your TRA, we recommend four things that you must first look at:

1. The scope of work, number of buildings, and the purpose of the assessment.
2. The type of environment with a description of each building and the type of business operation.
3. Operational hours, number of employees, contractors, vendors, and visitors on-site each day.
4. Asset identification and determining what security measures are currently in place to protect the assets, area crime data, and problem identification.

Next we have four things you should be looking for:

1. Threat identification
2. Probability of risk assessment
3. Impact assessment
4. Threat analysis/levels

Under Vulnerability Assessment there are four things to look for:

1. Current control measures identification
2. Control measures effectiveness
3. Identify exposure gaps
4. Vulnerability analysis level

Also, consider the vulnerability and the probability that an incident will occur and the impact the incident will have on the operation.

1. Risk analysis levels 2–10, low; 11–20, medium; 21–30, high
2. Priority risk based on risk profile

Closing the gap:

1. Examine mitigation options
2. Cost–benefit analysis
3. Residents risk analysis
4. Recommend a mitigation option

Four Classification of Pure Risk:

1. Personnel risk
2. Property risk
3. Liability
4. Risk arising from the failure of others

Data Collection: Data should include local history, intelligence, industry experience, or probability forecast. Examine the frequency of events and what can be done to remove or reduce the threat and probability of reoccurrence. Reassess at least annually and include revision data on all documents.

74. WHAT IS RISK ANALYSIS?

Risk analysis is a management tool, the standards for which are determined by whatever management decides they are willing to accept in terms of actual loss. To proceed in a logical manner to perform a risk analysis, it is first necessary to accomplish some basic tasks:

- Identify the assets that need to be protected (money, manufactured products, and industrial processes to name a few).
- Identify the kinds of risks (or perils) that may affect the assets involved (kidnapping, extortion, internal theft, external theft, fire, or earthquake).
- Determine the probability of risk occurrence. Here one must keep in mind that such a determination is not a science but an art—the art of projecting probabilities. Remember this rule: "Nothing is ever 100% secure."

Determine the impact or effect, in dollar values if possible, if a given loss does occur. (Charles A. Sennewald, Effective Security Management, 4th ed., 2003).

WHAT IS A RISK ASSESSMENT ANALYSIS?

Risk assessment analysis is a rational and orderly approach, and a comprehensive solution, to problem identification and probability determination. It is also a method for estimating the expected loss from the occurrence of some adverse event. They key word here is estimating, because risk analysis will never be an exact science—we are discussing probabilities. Nevertheless, the answer to most, if not all, questions regarding one's security exposures can be determined by a detailed risk assessment analysis.

75. ASSESSMENTS: QUALITATIVE VERSUS QUANTITATIVE METHODS

Many people think that the terms qualitative and quantitative can be used interchangeably, but they have different meanings.

Qualitative means that you are searching for underlying reasons for why things have happened (e.g., crime, accidents, injuries) and are looking for patterns. Many times when conducting a security risk assessment, it is beneficial to have informal focus groups to help you gain insight to problems of crime or disorder on the property being assessed.

Quantitative means that you are using numerical data that can be transformed into usable statistics. It is a means to measure data to formulate the facts and find patterns in the information. Collecting quantitative data is a very structured process. For example, collecting Uniform Crime Report (UCR) data, crime information from local law enforcement agencies, and using site incident reporting numbers would be considered quantitative methods.

76. DEFENSE-IN-DEPTH

Layered security is also known as defense-in-depth, and this principle is effective for both physical and logical securities. Defense-in-depth means that one single security is not enough to adequately protect assets and a series of complementary levels of security make up effective assets protection.

ASIS International defines layered security as "a physical security approach that requires a criminal to penetrate or overcome a series of security of security layers before reaching the target. The layers might be perimeter barriers; building or area protection with locks, CCTV and guards; and point and trap protection using safes, vaults and sensors."[3]

77. LAYERS OF PROTECTION ANALYSIS[4]

The security professional also may use varied levels of risk analysis to provide estimates of the event likelihood technique called Layers of Protection Analysis (LOPA). The LOPA also allows the risk to be estimated along various points throughout the incident sequence. In addition, it can provide quantitative estimates of the risk with which LOPA can be applied to hazardous events that have a consequence severity involving any type of scenario:

- Any facility or equipment damage or failures that may cause harm (i.e., may be either an internal or external explosion, or a detonation within the facility perimeter)
- Significant operations interruption (i.e., possibly a bomb threat, workplace violence incident, threat via the mail)
- Serious injury or fatality of an employee or staff (i.e., active shooter/active assailant)
- Any external injury or fatality to the community at large
- Significant environmental impact that affects everyone (i.e., gas or chemical exposure)

When LOPA is used by the security professional, they will begin with examining how causes lead to process deviations (or initiating events); this will assist with understanding how they propagate (also called "chain reaction" or domino effect). Hopefully, the security professional is able to determine if any enabling conditions (root causes) were critical to understanding the failed event, i.e., any inappropriate process deviation. In addition, the risk rank procedure that is performed will use a risk matrix for calculation purposes, and then the event risk is compared with the operations risk to determine whether additional risk reduction or mitigation techniques are required. Summers and Hearn[5] argue that when the process risk does not satisfy the chosen risk criteria then an

[3] ASIS, Protection of Assets Manual; 2006.
[4] Beaudry M. *Effective physical security*, 5th ed. Elsevier, Cambridge, MA; 2017.
[5] Summers AE, Hearn WH. Risk Criteria, Protection Layers and Conditional Modifiers paper; 2010.

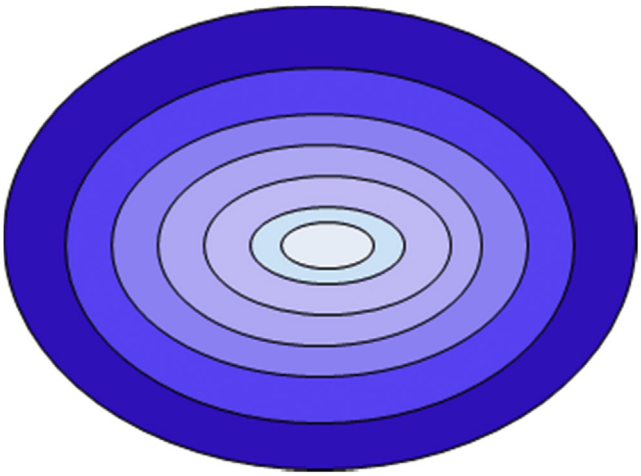


FIGURE 1

Typical lines of defense when designing layers of protection.

independent protection layer (IPL) is used to close the gap by reducing or mitigating the hazardous or harmful event frequency.[6] Initially, the main purpose of IPLs is to stop propagation of the hazardous event (think of it as a time delayed mechanism) and any probable harm that may result from the event. Generally, most security professionals will utilize an onion-skin concept (sometimes referred to as lines of defense or defense-in-depth), used to illustrate the typical order of IPL deployment. Should a scenario progress through the onion skin of IPLs, it is designed to prevent or reduce the impact on the process operation. Also, a key element of using these types of lines of defense is that it will cause time delays, or difficulties, or the propagation (sometimes called a hard target versus a soft target that does not use layers of protection). Using LOPA is exactly represented by the layers of an onion skin, sometimes called "lines of defense." The objective is to implement barriers that will result in time delays for the offender to get to a targeted area (Fig. 1).

Ultimately, the primary goal of any layers of protection design is to implement a plan that will add value to preventing or delaying (reduce or mitigate) any attempts to breaching a business environment successfully. Typically, most designs lack an overall full proof plan. However, LOPA will assist the security professional to design a safer environment that adds key lines of defense with manageable access control and supervisory procedures or measures (checks and balance technique). In addition, the LOPA design creates preventive and mitigation layers that add to mitigating events from occurring. In addition, a well-designed posture that proactively reduces or mitigates any type of hazardous event can have a high certainty of effectiveness.

[6] CCPS/AIChE, Layer of protection analysis: simplified process risk assessment, Concept series, New York; 2001.

Since risk is a function of frequency and consequence, the frequency estimation and the LOPA concept can provide different techniques in evaluating its acceptability. Typically, the consequence severity is used by security professionals to conduct an assessment of the potential likelihood of events for stricter frequency analysis. As mentioned previously, many security professionals may rely on the assessment of operating experience and incident history to make their determination, and they may use holistic factors that influence the severity (i.e., crime rates, types of crime data) including operating practices, layers of protection, and conditional modifiers that can alert or monitor a situations events. Historically, during the assessments, the security professional may consider reactive and response layers, i.e., actions that facility personnel must take to reduce or mitigate harm; this will sometimes be in addition to the proactive layers (i.e., closing and locking a door from the inside of an office or room). One other important issue to keep in mind is that each layer provides protection independent of each other; the use of these layers and the conditional modifiers are critical, since they are often interrelated. For example, an alarm annunciator system may be used to initiate evacuation of personnel, or a lockdown situation for occupants.

USING LAYERS OF PROTECTION ANALYSIS

When using risk analysis, the LOPA can also be incorporated to improve implementation of consequence estimation tools.[7] In addition to the consequence estimation tool, the risk analysis also depends on the estimated frequency of the hazardous event. Additionally, any error associated with the consequence severity estimate directly impacts the risk reduction measures. Most security professionals will find that using the LOPA is easy and flexible. When attempting to determine priorities based on the estimate of the hazardous event frequency, look carefully at those root causes of events that lead to the hazardous event and the possibility that the safety and security measures may fail. Security professionals will use experience to determine the right types of protection layers to utilize and use best practices to demonstrate the risk reduction or mitigation techniques that have worked when conducting previous risk analysis. Security professionals will need to determine the root causes (or initiating causes) and analyze those enabling conditions that result in process deviations (or initiating events). This is a critical part of risk analysis since by understanding the likelihood of the types of hazards that may occur and the conditions that enable them, security professionals can then estimate the initiating event frequency.

78. FIVE TECHNIQUES TO DEAL WITH IDENTIFIED RISKS

1. Risk Avoidance: This is the process by which you reduce the risk exposure by avoiding or eliminating the activities.

[7] Summers AE, Hearn WH. Risk criteria, Protection layers and conditional modifiers paper; 2010.

2. Risk Loss Reduction: This is reducing the risk by reducing the maximum amount of probable loss; utilizing other venues, personnel, equipment, etc., for the activity.
3. Risk acceptance: This is accepting the risk as it cannot be cost effectively reduced. However, all necessary attempts should be taken to monitor any increases in risk exposure to a preestablished level. Once that level is reached, there will be no other option but total removal of the personnel at risk.
4. Risk Transference: This is the use of contracts, insurance, disclaimers, and/or releases of claims to transfer the liability for the expected loss to other parties involved.
5. Risk Spreading: This is simply spreading the largest amount of risk over a larger part of the organization or activity by manipulating the sequence or size of the events or activities.

INSURANCE

This is the transfer of risk from one party to another in which the insurer is obligated to indemnify the insured for an economic loss caused by an unexpected event during a period of time covered by such insurance. Types of insurance vary from liability to crime/theft losses and fire. Rates are governed based on the frequency of claims and cost of each claim.

RISK MITIGATION STRATEGIES

- Risk avoidance
  - Removal
- Risk reduction
  - Decrease potential
- Risk spreading
  - Spread the risk
- Risk transfer
  - Insurance
- Risk acceptance
  - Acceptance
- Risk Avoidance
  - Risk is avoided when the *organization refuses to accept it*. The exposure is not permitted to come into existence. This is accomplished by simply not engaging in the action that gives rise to risk. If you do not want to risk losing your savings in a hazardous venture, then pick one where there is less risk. If you want to avoid the risks associated with the ownership of property, the do not purchase property but lease or rent instead. If the use of a particular product is hazardous, then do not manufacture or sell it. This is a negative rather than a positive technique. It is sometimes an unsatisfactory approach to

dealing with many risks. If risk avoidance were used extensively, the business would be deprived of many opportunities for profit and probably would not be able to achieve its objectives.

- Risk Reduction
  - *Risk can be reduced in 2 ways—through loss prevention and control*. Examples of risk reduction are medical care, fire departments, night security guards, sprinkler systems, burglar alarms—attempts to deal with risk by preventing the loss or reducing the chance that it will occur. Some techniques are used to prevent the occurrence of the loss, and other techniques like sprinkler systems are intended to control the severity of the loss if it does happen. No matter how hard we try, it is impossible to prevent all losses. The loss prevention technique cannot cost more than the losses.
- Risk Retention
  - Risk retention is the *most common* method of dealing with risk. Organizations and individuals face an almost unlimited number of risks, and in most cases nothing is done about them. When some positive action is not taken to avoid, reduce, or transfer the risk, the possibility of loss involved in that risk is retained. Risk retention can be conscious or unconscious. Conscious risk retention takes place when the risk is perceived and not transferred or reduced. When the risk is not recognized, it is unconsciously retained—the person retains the financial risk without realizing that he or she is doing so. Risk retention may be voluntary or involuntary. Voluntary risk retention is when the risk is recognized and there is an agreement to assume the losses involved. This is done when there are no alternatives that are more attractive. Involuntary risk retention takes place when risks are unconsciously retained or when the risk cannot be avoided, transferred, or reduced. Risk retention may be the best way. Everyone decides which risks to retain and which to avoid or transfer. A person may not be able to bear the loss. What may be a financial disaster for one may be handled by another. As a general rule, the only risks that should be retained are those that can lead to relatively small certain losses.
- Risk Transfer
  - Risk may be *transferred to someone who is more willing to bear the risk*. Transfer may be used to deal with both speculative and pure risk. One example is hedging; hedging is a method of risk transfer accomplished by buying and selling for future delivery so that dealers and processors protect themselves against a decline or increase in market price between the time they buy a product and the time they sell it. Pure risks may be transferred through contracts, like a hold-harmless agreement where one individual assumes another's possibility of loss. Contractual agreements are common in the construction industry. They are also used between manufacturers and retailers about product liability exposure. Insurance is also a means of transferring risk. In consideration of a payment or premium, by one party, the second party contracts to indemnify the first party up to a certain limit for the specified loss.

- Risk Sharing
  - This is a special case of risk transfer and retention. *When risks are shared, the possibility of loss is transferred form the individual to the group*. A corporation is a good example of risk sharing—a number of investors pool their capital, and each only bears a portion of the risk that the enterprise may fail.
  - A TRA will incorporate a combination of mitigation tools into the TRA.

79. ASSESSMENT OF COUNTERMEASURES

The other side of the inspection coin is the examination of existing countermeasures, usually protection programs and activities, originally set into motion to cure the known risks. The discovery of risks usually comes from conditions that are observable or comprehensible by virtue of what has happened, what is happening, and what could happen, whereas countermeasures are best assessed through analysis of the countermeasures activity itself. This analysis is usually accomplished by asking questions. The primary and most devastating question us "Why?" Every countermeasure and every security program should be subjected to the following questions:

- Why are we doing it?
- Must we do it at all?
- If we must, is there a better way?
- Is there a less expensive way?

80. SECURITY SYSTEM INTEGRATION

Assets are best protected when a security process is designed that integrates the appropriate mix of electronic, physical, and security procedures.

Many security systems are increasingly being equipped with network connectivity to enable them to share a facility's network infrastructure. Planning for, implementation, and management of converged security solutions often requires partnerships between physical security, IT security, and other corporate or organizational stakeholders.

To have effective security system integration:

- Security efforts must be coordinated.
- Redundant communication capabilities must be a part of the system.
- The security system should be properly maintained.
- The security system should be tested and audited.

An effective security system will have many components working together to achieve the desired level of protection, but first you have to determine the goals of security integration.

- Policies and Procedures: entry procedures, wearing IDs, report incidents.
- Electronic Security: integrated with all video surveillance and intrusion detection systems.
- Physical Barriers: door, locks, lighting, gates fences.
- Security Personnel: control processes, enforce policies, follow procedures.
- External Resources: police, fire, EMS (emergency medical services).

A Systems (holistic) approach to security systems address a total problem using:

- A vulnerability assessment: determine the excesses and deficiencies in existing security.
- Countermeasures: may be hardware, software, or people.
- Testing of the system: audit the system to see what changes need to be made.

81. KEY FACTORS IN AN ASSET PROTECTION PLAN

1. An adequate master plan to prevent losses from occurring.
2. Adequate countermeasures to reduce and limit the losses.
3. Management support of the plan.

82. SEVEN THINGS YOU SHOULD KNOW ABOUT PHYSICAL SECURITY INFORMATION MANAGEMENT

1. Physical Security Information Management (PSIM), created by middleware developers, designed to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface.
2. Basically it is used effectively when you tie in several smaller locations into the main unit. It collects and correlates events from existing disparate security devices and information systems (video, access control, sensors, analytics, networks, building systems, etc.) to empower personnel to identify and proactively resolve situations.
3. Locations are generally scattered across several states even internationally and linked together.
4. It provides consolidation; PSIM integration enables numerous organizational benefits, including increased control, improved situation awareness, and management reporting. Ultimately, these solutions allow organizations to reduce costs through improved efficiency and to improve security through increased intelligence.
5. Your large critical infrastructure is ideal for your server system design.
6. PSIM Software tells your security managers just about everything you need to know, even which door is ajar or which door has been opened. Many of the alarms and alerts that come into the security environment are not really threats. These need to be prioritized according to the risk, such as time of day, location of personnel, and a whole range of other critical factors. “Dynamic

alarm management" is required to find the "hot" ones that indicate that some action may need to be taken. Connected systems and automation of processes such as key personnel alerting, video verification, and Service Level Agreements will help to ensure that alarms/alerts are followed up quickly and in a relevant manner.

7. PSIM software must be scalable; it must provide redundancy to grow and adapt to change (marketing@cnlsoftware.com March, 2016).

83. DESIGNING SECURITY AND WORKING WITH ARCHITECTS

LEADERSHIP IN ENERGY AND ENVIRONMENTAL DESIGN

As with Crime Prevention Through Environmental Design (CPTED), some of the leadership in energy and environmental design (LEED) concepts complement security concerns, whereas others conflict with physical security principles. The LEED Green Building Rating System represents the US. Green Building Council's (USGBC's) effort to provide a national standard for what constitutes a "green building." Through its use as a design guideline and third-party certification tool, it aims to improve occupant well-being, environmental performance, and economic returns of buildings using established and innovative practices, standards, and technologies.[1] LEED is a voluntary building assessment tool that is most applicable to commercial, institutional, and high-rise residential construction. Owners, architects, and engineers must work together to strike a balance between building design objectives.

LEED looks at six basic categories: sustainable sites, water efficiency, energy and atmosphere, materials and resources, indoor environmental quality, and innovation and design process. Within each category, points are awarded for achieving specific goals. A total of 69 points is possible. A score of 26–32 points achieves basic certification, 33–38 achieves silver, 39–51 achieves gold, and 52–69 points achieves platinum certification. The LEED rating is awarded after the project has been documented by the USGBC.

Another goal in the LEED effort is to encourage more sustainable construction practices. LEED encourages manufacturers to provide materials that:

- Contain high recycled content and sustainable use raw materials
- Are manufactured close to the construction site
- Have low-volatile organic compound emissions
- Are designed to minimize energy consumption and packaging

CPTED PLANNING AND DESIGN REVIEW

One of the first priorities for implementing CPTED is to place it in the planning process of the organization or jurisdiction. School districts, housing authorities,

transportation systems, and local government all have fundamental responsibilities for public safety. It is necessary that a formal relationship between crime prevention and planning be established. Private companies and public utilities control extensive properties and huge labor forces. Each has a process for making decisions about new development and investment. The CPTED concept and process must be incorporated into these ongoing processes. Research has shown that it is the multidisciplinary team that creates a greater value when working on CPTED projects.

For communities and organizations, the CPTED process relates to and must be part of the following functions:

- *Comprehensive plans*: These determine the future patterns of land use and development. Comprehensive plans present the values of a community and a vision of what it will look like in the future. These plans establish goals and objectives for up to 50-year time periods. Crime prevention elements are clearly necessary in a community's comprehensive plan. Day-to-day decisions about problems and needs are improved by ensuring that they are consistent with comprehensive plans.
- *Zoning ordinances*: These are established to promote the health, safety, and welfare of the people by formally identifying the locations of land uses to ensure that activities are compatible and mutually supportive. Zoning regulations affect land uses, development densities, yard setbacks, open space, building height, location and amount of parking, and maintenance policies. These, in turn, will affect activities and routines that concern exposure to crime, surveillance opportunities, and the definition of space for territorial control.
- *Subdivision regulation*: This includes lot size and dimension, street and right-of-way locations, sidewalks, amenities, and location of utilities. These elements directly influence access to neighborhoods, reduction of pedestrian and vehicle conflict, street lighting, and connections with other parts of the community.
- Landscape ordinances: These govern the placement of fences, signs, and plant materials. They may be used to improve spatial definition, surveillance, access control, and way-finding. Hostile landscaping can make unwanted access to parking lots and private property less desirable. Landscape planting materials may also help to reduce graffiti by making large areas of walls inaccessible. Good horticulture improves the quality of life and helps to reduce exposure to crime.
- *Architectural design guidelines*: These guidelines specify goals and objectives for site and building performance. They will affect the location of activities and the definition of public and private space. The site decisions and plans for a building will directly affect opportunities for natural surveillance, pedestrian and vehicle access, way-finding, and links to adjacent neighborhoods or land uses.
- *Access for physically and mentally challenged persons*: These requirements generally improve accessibility and way-finding, but rarely consider the risk of victimization that may be created by the use of out-of-the way doors, hallways, or elevators.

Review Process

The work of builders, designers, and planners has long been affected by codes that govern nearly every aspect of a structure, except for security. Historically, a few jurisdictions enacted security ordinances, but most of these related to windows, doors, and locking devices. It is now becoming more common to find a local law or procedure calling for a full security or crime prevention review of plans before they are finalized. Nevertheless, it is still generally true that more attention is placed on esthetics, drainage, fire safety, curb cuts, and parking access than on gaining an understanding of how a building or structure will affect the area in terms of security. A CPTED design review process must be established within communities and organizations to ensure that good planning is being conducted.

The manner in which physical space is designed or used has a direct bearing on crime or security incidents. The clear relationship between the physical environment and crime is now understood to be a cross-cultural phenomenon, as recent international conferences on CPTED have disclosed the universal nature of human/environment relations. That is, despite political and cultural differences, people basically respond the same way to what they see and experience in the environment. Some places make people feel safe and secure, whereas others make people feel vulnerable. Criminals or other undesirables pick up on the same cues. They look at the environmental setting and at how people are behaving. This tells them whether they can control the situation or run the risk of being controlled.

Conclusion: Achieving LEED gold does more than just showcase a commitment to the environment. It is a creative strategy that produces significant energy and maintenance efficiencies and cost savings.

Source: Handbook of Crime Prevention and Loss Prevention, Butterworth-Heinmann, 2012.

84. PADLOCKS

The distinguishing feature of padlocks is that they use a shackle rather than a bolt as the device that fastens two or more objects together. The shackle is placed through a hasp that is permanently affixed to the items to be fastened. Three methods are commonly used to secure the shackle inside the lock body. The simplest and least secure method is to press a piece of flat spring steel against an indentation in the shackle. When the key is inserted, it rotates to spread the spring releasing the shackle. This is a locking method commonly found on warded padlocks. More rarely it is found on tumbler-type locks, but it is found occasionally on the less expensive models.

A slightly more secure method uses a locking dog. The dog is spring-loaded and fits into a notch cut into the shackle. The key is used to retract the dog, permitting the shackle to be withdrawn. Both these spring-loaded mechanisms are vulnerable to attacks that take advantage of the fact that the locking device can be forced back against the spring by a suitable tool. Shimming and rapping are common techniques used to open them. Often a stiff wire can be pushed down the shackle hole to engage

and force back the spring or locking dog. Spring-loaded padlocks should not be used where reasonable security is required.

Positive locking techniques do much to reduce the vulnerability of padlocks to these types of attacks. The most common positive locking method uses steel balls inserted between the cylinder and the shackle. In the locked position, the ball rests half in a groove in the cylinder, and half in a notch cut into the shackle. In this position, the shackle cannot be forced past the steel ball. When the cylinder is turned to the unlocked position, the groove deepens permitting the ball to retract into the cylinder when pressure is put on the shackle. This releases the shackle and opens the lock. These locks are designed so that the key cannot be removed unless the lock is in the locked position.

Padlocks are vulnerable to attacks at several better points. The shackle can be pried out of the lock by a crowbar or jimmy, or it can be sawed or cut by bolt cutters. The casing can be crushed or distorted by hammering. Modifications have been incorporated into better padlocks to reduce their vulnerability to these approaches. Heavy, hardened steel cases and shackles are used to defeat cutting and crushing. Rotating inserts and special hardened materials are used to prevent the sawing of shackles. Toe and heel locking is used to prevent prying.

High-security padlocks are large and heavy, using hardened metals in the case, and a thick, hardened, and protected shackle. Positive locking methods are always used. As little of the shackle is exposed to attack as possible in the locked position. This is the "shackle-less" padlock, which is designed so that a "locking bar" that is contained entirely inside the case is used in the place of an exposed shackle. This is sometimes called a "hasp lock" rather than a padlock.

A padlock is, however, no better than the hasp it engages. Hasps offering reasonable security are themselves made of hardened metals. They must be properly mounted on solid materials so that they cannot be pried off. In the locked position, no mounting screw or bolt should be accessible. Padlocks and hasps should always be considered as a unit. There is no point in mounting a high-security padlock on an inferior hasp. The hasp and lock should always be of approximately the same quality. Where they are not, the complete device is only as good as its weakest member.

Source: Edgar JM, CPP, McInerney WD, Finneran ED, Hunter JE. The Use of Locks in Physical Crime Prevention. Effective Physical Security, 5th ed.; 2016 B-H.

85. WHAT IS A MASTER PLAN?

A Security Master Plan is a document that delineates the organization's security philosophies, strategies, goals, programs, and processes. It is issued to guide the organization's development and direction in these areas in a mann 1 er that is consistent with the company's overall business plan. It also provides a detailed outline of the risks and the mitigation plans for them in a way that creates a 5-year business plan.[8]

[8] Giles D. Output Convergence and International Trade: Time-Series and Fuzzy Clustering Evidence for New Zealand and Her Trading Partners; 2001.

86. SECURITY MASTER PLANS

A Master Plan for Security should be a part of the Operational Master Plan and Mission Statement for the organization. Master planning is a catalyst for defining a vision for security that touches all aspects of service delivery including technology, emergency management, and IT security.[9]

Information needed to develop a Master Plan for Security includes:

- General background information on the company
- An organizational chart for the management of the facility
- A copy of the post orders
- A copy of the site security manual
- Blueprints of the facilities to be reviewed
- Copies of any security-related procedures or practices, including information protection
- Copies of incident reports for the past 2 years
- Copies of any incident summary or analysis data
- Copies of any crime statistic data on hand
- A copy of the contract guard contract, if applicable
- A copy of any other security-related contracts, such as confidential destruction
- The current staffing of the security organization by rank
- A listing of any cash operation on-site including how much cash is kept in hand
- A listing of any precious metals stored on-site and their value
- Any unique security-related issues you should be aware of
- The location of any high-security areas on-site and why they are so considered
- Security system information, brand name, and model or level
- Type of lock and key system(s) in use at the facilities

87. HOW TO DESIGN A 5 AND 10-YEAR SECURITY PLAN

THE FIRST 5 YEARS

For example, let us start with the garage or your parking areas and any other areas that need updating or replacement. Blue light (emergency) phones in your parking lot, intercoms or emergency call stations in your garage, adequate lighting, fire detection, notification and suppression systems in the garage, and security surveillance systems are components to include in a 5-year plan. Upgrading these components is not an easy project unless you have effectively budgeted for this.

When we developed our first 5-year plan, we evaluated what was currently in place. Several cameras in the garage were not working properly so we switched to digital and replaced the units with HD PTZ (high definition & pan tilt & zoom)

[9] ASIS, Highlight of Presentation by David Giles, ASIS, Anaheim, CA 2015.

cameras with HD monitors. All the garage intercoms except for two were inoperable because of water damage and had to be replaced. Lighting was not at the recommended levels, so rather than invest in adding more fixtures, we had light-emitting diode lighting installed in the garage and the parking lots. Our plan projected the ROI (return on investment) on the lighting investment to help with future security upgrades for the organization.

Access control and access cards were an issue because the organization employed approximately 1000 employees, but over 1500 active cards were in the system. To compound this issue, we were initially unable to access activity reports. With the help of the HR and managers, each department within the organization was audited, and terminated employees were removed from the system and their access cards deactivated. Fortunately, none of the access cards had been used by terminated employees. The original card access control system did not have the expansion capabilities that were needed, so we were able to upgrade to a new system that we could integrate with video surveillance.

It took 5 years of careful budgeting and innovative security strategies to repair the existing security components and upgrade totally inoperable or outdated systems. The physical security program had not been effectively managed, so we put in place scheduled programs to service and reevaluate each security component on-site. Some things can be done as problems surface, but it is much better to be proactive and schedule maintenance and service before there are issues. For example, the video surveillance system was composed of all analog, monochrome cameras, with no plans to upgrade when inoperable cameras were replaced. It did not make sense to keep investing in old technology. As the old cameras were replaced, we were able to have monitor images that were of better quality, and it also increased our storage capabilities.

TECHNOLOGY

Technology is not the answer to security. It should be considered one component in the security process. Many times, organizations are not protected because they rely on technology that is outdated or they have security officers who do not know how to operate camera systems or access control because they have never been trained. This creates a false sense of security for the organization. Two good examples are as follows:

- It was observed that 50% of the card readers were not working properly. Management and security officers thought the card readers were operating properly, but they had never been checked. No reports had ever been generated, and no audits were done to test the integrity of the system.
- Management believed that the video surveillance system was an effective component of their security program, but it was not a monitored system and many of the images had poor resolution, so it could not be used for investigations or access control issues.

An effective security system will have many components working together to achieve the level of security that is desired, but effective management of these systems and proper training are essential.

THE NEXT 5 YEARS

What causes change? Standards, guidelines, regulations, best practices, audits, mergers, a crisis (unfortunately), and budgeting for change.

What if I gave you $500,000.00 for your security program? How would you spend it? How would you prioritize the needed changes? What risks is the organization willing to take? What risks should be mitigated? It is important that this is an informed decision, so we recommend that a security risk assessment be conducted first to identify inadequate components in your security program as well as vulnerabilities. After vulnerabilities are identified, you must budget them into first a 5-year plan and then a plan for the next 5 years. What should you do first and what can be scheduled and budgeted for at a later time? Vulnerabilities must be ranked in order of critical need to the organization. Any upgraded system must have expansion capabilities that correspond with the projected growth and anticipated changes for the organization. You should also invest a significant amount of money in training because it does not make sense to have the latest technology and systems if no one knows how to effectively use it.

TRAINING

The *Business Dictionary*[10] defines training as, "Organized activity aimed at imparting information and/or instructions to improve the recipient's performance or to help him or her attain a required level of knowledge or skill."

There is good training and there is training that is not so good. Good training follows a logical format, and it is effective in relaying information in a manner that can be easily be understood by the students. For example, security officers must understand the security components that they will be operating and are responsible for—most often access control and video surveillance systems. Ensure you have quality training programs that are being delivered effectively. The crux of the matter is, many trainers do not have *training* in conducting training. This is a fact that is quite ironic. The bottom line is, pull your security program together. Decide who should be trained and who will conduct the training.

88. MASTER PLANNING: PHYSICAL SYSTEMS

The phrase "Master Plan" is more than just an expression. However, it also applies to your Physical Security Systems.

1. Intrusion alarms
   - **a.** What is it you intend to alarm and protect?
   - **b.** Who will monitor the system?
   - **c.** What components do you intend to use?
   - **d.** How will this alarm fit in your overall plan?

[10]The Business Dictionary; 2016. www.BusinessDictionary.com.

2. Access control
   a. Is it needed or a requirement?
   b. Will it be a stand-alone or part of a bigger package?
   c. Consider the overall design, the mixture of biometrics.
   d. Badge control must be a part of your plan.
3. Security surveillance systems
   a. Consider the very latest in technology and equipment because in 5 years it is no longer state of the art.
   b. Consider the monitoring and response as well as how it will be administered.
   c. HD, 1080p, multiscreen digital recording; interior, pan and tilt—consider how and what this system is to achieve.
4. Control room or front
   a. Consider how it is to be laid out.
   b. Do not stick it all in a closet.
   c. Define the space and define the usage.

89. ACTIVE SHOOTER/ACTIVE ASSAILANT RESPONSE

As part of a Security and Risk Assessment follow-up, you may be asked to assist with the development of an Active Shooter Response Plan. The Department of Homeland Security has some options as do other private training organizations. Regardless of the program you choose, it is important to be proactive and conduct training and exercises with local first responders.

According to the Federal Bureau of Investigation, 56.3% of active shooter incidents over the past decade ended with the gunman committing suicide or fleeing the scene. Another 28.1% of the threats ended when law enforcement engaged the shooter in gunfire. Relatively few incidents, just 13.1%, ended after unarmed citizens restrained the shooter.[11]

There are several options, but Battelle, a company headquartered in Columbus, Ohio, conducts research and development, designs and manufactures products, and delivers critical services for government and commercial customers. Battelle's SiteGuard Active Shooter Response (ASR) is designed to save lives by *detecting*, *locating*, *and responding* to gunfire—automatically—to reduce response time in the first critical and chaotic minutes of an incident.

The system has a series of interior and exterior sensors placed throughout a building that can detect gunfire and pinpoint its location. The computer system automates, accelerates 911 calls, and triggers building lockdown to deny or delay shooter access to additional victims. The ASR system also has the technology to access the video surveillance system so that law enforcement can view live video of the event to better respond (http://www.battelle.org/our-work/homeland-security-public-safety/battelle-siteguard-active-shooter-response).

In addition, it should be noted that ASIS and NFPA are designing a standard on the topic of Active Shooter.

[11] FBI; 2014. https://www.fbi.gov/file-repository/active-shooter-study-2000-2013-1-1.pdf.

PART

Crime and Crime Prevention Techniques

3

90. THE CRIME PREVENTION TRIANGLE[1]

The concept of the crime prevention triangle states that for a crime to occur, all three elements of the triangle must exist: *Desire*, *Ability*, and *Opportunity*.

If any one of these elements is eliminated, a crime cannot occur.

WHAT IS NECESSARY FOR A CRIME TO OCCUR?

1. The *desire* or motivation on the part of the criminal to commit the crime.
We cannot remove a criminal's *desire* to commit a crime. If someone really wants to commit a crime he or she will.
2. The skills, tools, and *ability* needed to commit the crime.
We cannot affect the *ability* of a criminal to commit a crime. A criminal will find a way to commit a crime if he or she wants to.
3. The *opportunity* to commit the crime.
We can remove the *opportunity* for a criminal to commit crime. Opportunity is the only element of the crime prevention triangle that we can affect.

91. ANTICIPATION OF CRIME RATE CHECKLIST

Crime data are usually obtained from the local police department and also from incident reported to the security department. The *CAP Index* is another way of determining the level of crime within a one-mile radius of your location.

As you do with any security survey or risk assessment, your first step is to consult with the customer and the occupants of the facility or complex. It is important

[1] http://www.citynmb.com.

Physical Security: 150 Things You Should Know. http://dx.doi.org/10.1016/B978-0-12-809487-7.00003-6

that you identify their concerns about security. Additionally, areas must be identified where security-sensitive or high-value items are located, such as vaults or safes, IT equipment, as well as telephone and data room.

It is important that you identify the main crime targets and then access the level of protection required. Examine the facility or complex. From that survey, the building characteristics and personality can tell you how the structure has been used or abused and what is needed to determine an effective level of security that is also feasible and affordable.

To determine the level of security that is required in a particular location, a list of some of the information that you will need is provided:

- Are there "reasonable" security policies and procedures that are in place and are they enforced?
- Does lighting meet illumination recommendations, and is it evenly distributed to prevent dark areas?
- Is there cash being handled within the facility that needs to get to the bank, or is there an ATM on-site?
- Is there a concentration or an even distribution of valuables within the complex? Decide on the area most vulnerable to criminal attack, and craft your recommendations to harden those targets.
- Reduce entrances to a minimum, thereby reducing and centralizing movement of staff and visitors. It is important to note that you cannot block or delay egress from a building.
- What is the crime risk in the area?
- Are there "hot spots" or "crime magnets" located close by?
- What is the level of police patrol and law enforcement activity in the area?
- To estimate response time, what are the distances from the complex to the local police and fire stations?
- Do on-site functions, materials, and supplies, comply with local, state, and federal standards?
- Who is responsible for maintenance and custodial services?
- Are there security officers on-site? If not, who will secure the complex day and night? Are they dependable, intelligent, well-trained, and reliable?
- Make note of employee behavior on the site.
- Get input from employees about whether or not they "feel" safe. If not, where do they feel most vulnerable?

92. CRIME REPORTING AND CRIME ANALYSIS

CRIME REPORTING[2]

We are going to discuss three annual publications that document crime statistics in the United States:

1. Crime in the United States—Uniform Crime Reporting (UCR) The Summary System

[2] https://www.fbi.gov/about-us/cjis/ucr/ucr.

2. The National Incident-Based Reporting System (NIBRS)
3. National Crime Victimization Survey (NCVS)

Crime in the United States—Uniform Crime Reporting The Summary System

The UCR began in 1929 and is administered by the Federal Bureau of Investigation to collect data on crimes reported to law enforcement. UCR crimes are categorized as either violent or property crimes that are known as Part I offenses. These data are used to measure the level and scope of crime occurring throughout the nation. The eight offenses listed are chosen because they are serious crimes, they occur with regularity in all areas of the country, and they are more likely to be reported to law enforcement.

Violent Crime: defined in the UCR as an offense that involves force or threat of force.

Violent crime is composed of four offenses:

1. Murder and nonnegligent manslaughter
2. Forcible rape
3. Robbery
4. Aggravated assault

Property Crime: defined in the UCR as theft offenses involving the taking of money or property, but there is not force or threat of force against the victims.

Property crime is composed of four offenses:

1. Burglary
2. Larceny-theft
3. Motor vehicle theft
4. Arson

The National Incident-Based Reporting System

The NIBRS, an incident-based reporting system began collecting data in 1991 from law enforcement agencies (local, state, and federal) on each single crime occurrence.

- There are 22 offense categories made up of 46 specific crimes called Group A offenses.
- There are 11 categories for which only arrest data are reported, which are called Group B offenses.

Comparing UCR and the NIBRS Data:

- The NIBRS has more detail than traditional Summary (UCR) reporting.
- The NIBRS reports on 46 crimes known as Group A offenses. The Summary system collects offense information on eight crimes known as Part 1 Offenses.
- The NIBRS uses an updated definition of rape to include both male and female victims. In the Summary system, only females can be rape victims.

- The UCR Program (Summary System) uses the "Hierarchy Rule" to govern multiple offense reporting.
- The NIBRS reports each crime as a separate offense.
- The UCR Program (Summary system) has two crime categories: Crimes Against Persons and Crimes Against Property.
- In the NIBRS, there is a third category, Crimes Against Society (e.g., drug or narcotic offenses).
- The NIBRS collects information about crimes committed using a computer. The Summary system does not.

National Crime Victimization Survey

The NCVS, which began in 1973, is administered by the Bureau of Justice Statistics and provides a detailed picture of crime incidents, victims, and trends. Data are collected on crimes suffered by individuals and households, whether or not those crimes were reported to law enforcement. Victims describe the impact of crime and characteristics of violent offenders.

CRIME ANALYSIS

Crime analysis utilizes a set of quantitative and qualitative techniques to analyze data valuable to police agencies and their communities. It includes the analysis of crime and criminals, crime victims, disorder, quality-of-life issues, traffic issues, and internal police operations, and its results support criminal investigation and prosecution, patrol activities, crime prevention and reduction strategies, problem solving, and the evaluation of police efforts.[3]

Crime analysis is a critical first step in determining the need and scope for crime/loss prevention programs and also for correctly identifying and reporting problems.

Questions that are commonly asked are:

- Is crime up or is it down?
- Compared to whom and what?
- Is the local crime rate up, but the crime rate in your area down?
- What if you have a low crime rate in a high crime area?
- How do you get such information?

Police departments break crime down into areas, zones, or beats. Each area, zone, or beat is given a number. For instance, they may be numbered from 1 to 8, and if you are located in area, zone, or beat 6, you will want to know how the crime in your area compares with that in other areas, zones, or beats. To find this data, you must have relevant and reliable information. Crime analysis programs sometimes fail not because of the problems or crimes in a particular area, zone, or beat have not been properly identified.

[3] http://www.iaca.net/Publications/Whitepapers/iacawp_2014_02_definition_types_crime_analysis.pdf.

Crime Intelligence Analysis

Crime intelligence analysis is the analysis of data about people involved in crimes, particularly repeat offenders, repeat victims, and criminal organizations and networks. Crime intelligence analysis may use police record data as a starting point, but the crux of the process involves the confidential collection of information—"intelligence"—about individuals and networks, with associated concerns related to data security, access, and privacy, and the subsequent transformation of that information from data into intelligence through analysis.[4]

Crime Problems

Assume you have had as many as 12 burglaries in a particular neighborhood in your community. In each of the burglaries, entry was gained by forcing open a rear, sliding glass door. Items stolen include computers, cameras, CD's, stereos, video system and games, small televisions, clothing, and other miscellaneous items. What is most important in these particular burglaries is what was *not* stolen, such as valuable works of art, large flat screen TVs, silverware, or jewelry. None of the homes burglarized had their property marked or knew the serial numbers of the stolen items. All these burglaries occurred during the day when no one was home. These burglaries give you quite a bit of information to work with and follow-up on. Your results or conclusions may not always be obvious initially, but you will have to gather and develop more information and find data to determine the common denominators in each of the burglaries.

We cannot say enough about how important a follow-up visit is to a victim of crime. You may be given information that was not available at the time when the crime was reported. It may have been discovered later and would not be reported at all if you had not followed up with the victim. For instance, if cash was taken from a locked safe, it indicates a degree of knowledge. A note discovered that was not initially reported may be a critical piece of evidence.

Crime Trends

As you read crime reports, look for new items and current issues, and when you figure out how the crime was committed, only then can you develop a plan to prevent it from happening again. You may want to chart each crime. How were the targets selected? What was the escape route? How were the stolen items disposed of? Try to think the way the criminal was thinking. Where will the next crime be committed? Which neighborhood will the criminal pick next?

93. SITUATIONAL CRIME PREVENTION

The goals of Situational Crime Prevention are to reduce the opportunities for criminals to commit crimes, change the ways criminals think about whether or not they will be apprehended and prosecuted, and make it seem more difficult and less rewarding for a criminal to commit crime.[5]

[4] http://www.iaca.net/Publications/Whitepapers/iacawp_2014_02_definition_types_crime_analysis.pdf.
[5] http://www.popcenter.org/25techniques/.

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocation	Remove Excuses
1. *Target harden*: • Antirobbery screens • Physical locks for PCs	6. *Extend guardianship*: • "Cocoon" neighbourhood watch • Staff chaperoning of visitors	11. *Conceal targets*: • Gender-neutral phone directories • Minimize ID of offices	16. *Reduce frustrations and stress*: • Efficient queues and polite service	21. *Set rules*: • Harassment codes • Information security policies
2. *Control access to facilities*: • Entry phones • Swipe cards for office access	7. *Assist natural surveillance*: • Improved street lighting • Open plan offices	12. *Remove targets*: • Removable car radios • Clear desk and computer screens	17. *Avoid disputes*: • Reduce crowding in pubs	22. *Post instructions*: • "No Parking"
3. *Screen exits*: • Export documents • Reception desks	8. *Reduce anonymity*: • Taxi driver IDs • ID tags for staff	13. *Identify property*: • Cattle branding • Property marking	18. *Reduce emotional arousal*: • Controls on violent pornography	23. *Alert conscience*: • Roadside speed display boards
4. *Deflect offenders*: • Street closures • Segregation of duties	9. *Utilize place managers*: • Two clerks for convenience stores • Management supervision	14. *Disrupt markets*: • Monitor pawn shops	19. *Neutralize peer pressure*: • Disperse troublemakers at school	24. *Assist compliance*: • Easy library checkout • Security education for staff
5. *Control tools/weapons*: • Disabling stolen cell phones • Deletion of access rights for exemployees	10. *Strengthen formal surveillance*: • Security guards • Intrusion detection systems	15. *Deny benefits*: • Ink merchandise tags • Encryption	20. *Discourage imitation*: • Censor details of modus operandi • Prompt software patching	25. *Control drugs and alcohol*: • Alcohol-free events

When you think about Situational Crime Prevention, remember the acronym, SWOT (strengths, weaknesses, opportunities, threats). SWOT is a useful technique to help you understand Situational Crime Prevention, or in other words, the strengths and weaknesses in a program, identifying where opportunities exist and identifying the threats that may be encountered.[6]

Source: The Situational Crime Prevention Chart was prepared by Ronald V. Clarke.

94. "IF YOU SEE SOMETHING, SAY SOMETHING"

"If You See Something, Say Something" is a "national campaign that raises public awareness of the indicators of terrorism and terrorism-related crime, as well as the importance of reporting suspicious activity to state and local law enforcement."[7]

95. DETERRENTS

When the word "deterrent" is used as an adjective; it means "acting to stop or prevent," and when it is used as an adjective, it is defined as, "something that prevents or blocks."[8]

CATEGORY A

- Security surveillance system used to prevent crime in private and public locations
- Crime Prevention Through Environmental Design (CPTED) principles and concepts
- Defensible Space principles and concepts
- Situational Crime Prevention principles and concepts
- Lighting that meets standards and design by increased visibility
- Biometrics and access control to specific areas
- CPTED design
- CPTED security landscape principles
- Signage or visible security signs
- Padlocks, door locks, and door viewers (peep-holes)
- Intrusion alarms and alarm signage
- Security surveillance systems (closed-circuit televisions)
- Security awareness programs
- Planters and thorny bushes
- Bollards or barricades closing down streets

[6] Fennelly LJ. *Effective physical security*, 5th ed. Elsevier, Cambridge, MA; 2017.
[7] https://www.dhs.gov/see-something-say-something/about-campaign.
[8] http://www.yourdictionary.com/deterrent.

- Barking dog, inside, or outside
- Vehicle in driveway
- Area traffic and no escape routes
- Policies and procedures
- Training programs

CATEGORY B

- Security officers armed and unarmed in private functions, i.e., hotel door man, bus drivers, ticket sellers or ticket takers, or conductors.
- Police officers in uniform and armed security who may deduce that a crime is about to be committed and deter the incident by their presence.
- Security officer patrolling the parking lots of hotels, hospitals, and retail locations, protecting corporate assets and customers.
- Guardian Angels patrolling streets, neighborhoods, and subways.
- People in the area.
- Crime Displacement Theory by target hardening and moving soft targets to another location.

CPTED strategies are as follows:

1. Natural access control
2. Natural surveillance
3. Territorial reinforcement[9]

The CPTED Security Landscape principles are as follows:

1. For natural surveillance cut back bushes to a height of 3 feet.
2. Cut back the tree branches 8 feet from the ground.
3. Chain link fence height 6–8 feet with three strands of barbed wire.
4. Height of a stone wall should be 8 feet.
5. There should be at least 10 feet of clear space on both sides of the fence and wall.[10]

Defensible Space: This concept was developed in the public housing environment. It is similar to CPTED strategies.[9]

Environmental security differs from CPTED in that it uses a broader range of crime control strategies including social management, social media, target hardening activity support, and law enforcement.

Situation Crime Prevention incorporates other crime prevention and law enforcement strategies in an effort to focus on place-specific crime problems.

Results and Objectives:

- Reduce violent crime
- Reduce property crime

[9] Crowe, TD, Fennelly, LJ. *Crime prevention through environmental design,* 3rd ed. Elsevier, Boston, MA; 2013.

[10] Broder JF. *CPP risk analysis and the security survey*, 3rd ed. Elsevier; 2006.

- Displace crime
- Eliminate the threats and risks
- Reduce the likelihood of more incidents
- Eliminate vulnerabilities and protect assets

Risk Management is defined as "the process by which an entity identifies its potential losses and then decides what the best way is to manage these potential losses."[11]

1. Risk: exposure to possible loss (i.e., fire, natural disasters, product obsolescence, shrinkage, work stoppages).
2. Security managers are primarily interested in crime, shrinkage, accidents, and crises.
3. Risk managers generally are more focused on fire and safety issues.
4. Pure Risk: risk in which there are no potential benefits to be derived (i.e., earthquake, flood).
5. Dynamic Risk: risk that can produce gain or profit (i.e., theft, embezzlement).
6. Possible Maximum Loss: maximum loss sustained if a target is totally destroyed.
7. Probable Maximum Loss: amount of loss a target is likely to sustain.

96. RESIDENTIAL SECURITY

The crime risk to a residence may be reduced either by measures that decrease its vulnerability or measures that reduce the *crime pressure* in the area. The reduction of crime pressure is largely a social problem and a public policy concern. The vulnerability of a residence, on the other hand, is a particular concern, to usually be addressed by its owner or occupants of the home.

Security countermeasures are applied to a residence either to reduce the crime risk by decreasing its vulnerability or to reduce the probable cost and impact of a crime if it does occur. To determine the benefits and cost-effectiveness of a security measure, the crime risk must be measured in terms of dollars. This necessitates a measure of the probable cost of a random crime to the particular residence, fully reflecting the anticipated nature of the criminal damages (e.g., theft or personal injury) and the potential amount of these damages. Security measures may reduce vulnerability, thereby reducing crime risk, reduce the anticipated loss per crime, or in some cases, both. In all cases, their impact on the risk of loss will vary directly with the crime pressure.

Most countermeasures affect security in more than one way. Some of these effects maybe positive and others may be negative. The effectiveness of a security countermeasure depends on its impact on each aspect of a residence—or, put differently, on each of the crime-attracting characteristics that contribute to the vulnerability of the residence.

[11] Broder JF. *CPP risk analysis and the security survey*, 3rd ed. Elsevier; 2006.

HOME SAFETY AND SECURITY[12]

- Your house or residence number should be visible from the street.
- Install deadbolt locks on good-quality doors/door frames.
- All windows should have operational locks.
- All windows should be covered and there should be no views inside your house.
- Do not hide keys outside your home. Instead, give a key to a trusted neighbor.
- You should have sufficient exterior lighting around your home with no broken or damaged fixtures.
- Shrubs and bushes should be no higher than 36 inches and set back 1 yard from walkways so that they do not obstruct windows, doors, or walkways.
- Tree canopies should be trimmed up to 8 feet and should not obstruct exterior lighting.
- Ensure that no landscaping materials, such as loose gravel and stones, can be used as weapons.
- Earth berms should not create a visual obstruction and should be no higher than 2½ feet.
- Make sure landscape features do not provide a means of access onto the property or into your house.
- Graffiti or other signs of vandalism should be removed/repaired as soon as possible.
- Ensure your property is well maintained—the grass mowed and no trash or debris.
- If you have concerns, request for a police officer to perform a security survey of your home.
- If you decide to buy a weapon, consider pepper mace instead of a gun.
- If you do purchase a gun, get proper training and keep the gun under lock and key—especially if you have children. More children are killed by a weapon in the home than burglars.
- Have a "rally point," such as a trusted neighbor's house that is designated ahead of time if you must flee your house. Have your children practice going there and make sure the neighbor knows about it.

What to do at home when someone is breaking in

- Have a front and back escape route from your house. Ensure that no doors are blocked.
- Decide if you will fight or flee. Most police officers recommend fleeing and if you do flee, make sure everyone is out. Take your cell phone if possible, and meet at your rally point.
- If you have no escape route, consider going out a window. If you cannot get out of a door or a window, lock yourself in a room and barricade the door with furniture, if possible. Call the police.

[12] Cooper C, Perry M. LMPD Crime Prevention Forum. *Safety and security tips*. 2015.

What to do if you return home and suspect your house has been broken in to

- *DO NOT ENTER!!* Armed, violent criminals may be inside. They may kill you if you confront them!
- Call the police and have them check the house.

Weapons in the home

- If you are untrained, the weapon most police officers recommend for personal defense inside and outside of the home is *Pepper Mace*. It can disable or temporarily blind someone, but if it is used against you or your child finds it, no one will be seriously injured or killed.
- The biggest danger of having a gun in the home is that a child will play with the weapon and accidentally shoot someone or a young person will use it for an impulsive act, such as suicide.
- Another serious concern is that an assailant will disarm you and use the weapon against you.
- Stun guns are expensive, require maintenance, and do not always work properly. They also require that you to be in close contact with your assailant.

The aforementioned facts are common sense and practical steps that you can take to reduce the risk of crime or a dangerous incident occurring at your home. We recommend monitored intrusion detection systems (alarms) for residential security, possibly the use of cameras for video surveillance outside the residence, and also monitoring doors or vulnerable locations inside the home, but not in locations where there is a reasonable expectation of privacy.

97. SPACE

The continuum of space within a residential complex (that is, a property consisting of one or more buildings containing dwelling units and associated grounds or, more broadly, a neighborhood consisting primarily of residential uses) may be divided into four categories:

- *Public*: Space that, whatever its legal status, is perceived by all members of a residential area or neighborhood as belonging to the public as a whole, which a stranger has as much perceived right to use as a resident.
- *Semipublic*: Space accessible to all members of the public without passing through a locked or guarded barrier. There is thought to be an implied license for use by the public, and strangers will rarely be challenged. Generally associated with multifamily housing.
- *Semiprivate*: Space restricted for use by residents, guests, and service people on legitimate assignments. In multifamily housing, usually secured by protection officers (or doormen), locks, or other forms of physical barriers. Strangers can be expected to be challenged as potential trespassers.

- *Private*: Space restricted for use by residents of a single dwelling unit, their invited guests, and service people, with access generally controlled by locks and other physical barriers. Unauthorized use is always challenged when the opportunity for challenge presents itself.

At times you may view a property as either defensible or defenseless, based upon its characteristics. Recently, while conducting an assessment we discovered that crime was high in 2012 and continued to rise in 2013. No follow-up was done to any of the 2012 incidents, so many reoccurred in 2013. The opportunity for a crime to occur was never reduced or corrected and no deterrents were put in place. Criminals see areas of opportunity when they conduct their own assessments to determine whether or not to target a particular location. Many times we do not give criminals enough credit for assessing the risks of being caught. Certainly, some "not-so-smart" criminals will be caught, but what about those whose crimes law enforcement did not solve? Crime patterns have to be identified and then be followed up with proactive recommendations and measures.

While doing a security assessment, we had an administrator show us his office and tell us how secure his office area was, about the newly implemented security policies and procedures and the new door and window locks. The following morning when he came to work, there was a note on his desk from us—telling him how we got to his office space by using an unsecured freight elevator. To identify vulnerabilities and put appropriate countermeasures in place, study the scene carefully, inspect the area, ask the right questions, look for clues, discover the facts, conduct a crime analysis, and above all, think like the criminal who wants to commit a crime.

Many times, a victim will ask, "How did he get inside our space?" Most often, it is through an unlocked door or window. Ensure that positive crime prevention solutions are put into place and that they are utilized. The best locks available can only secure property if they are used.

In today's society, we tend to consider all areas outside the residence as semipublic or public space. CPTED encourages converting semipublic space to semiprivate space. Residents tend to ignore crime that occurs in semipublic or public spaces, by taking an "I don't want to get involved," attitude. The CPTED strategy can be applied in a very positive way, and will result in a reduction in crime and the fear of crime, as well.

CPTED STRATEGIES

The previous discussion suggests a series of general design strategies that can be applied in any situation to improve natural access control, natural surveillance, and territorial behavior.

- Provide a clear border definition of controlled space.
- Provide a clearly marked transition from public to semipublic to private space.
- Locate gathering areas in places with natural surveillance and access control away from the view of potential offenders.
- Place safe activities in unsafe locations and unsafe activities in safe locations.

- Provide natural barriers to conflicting activities.
- Improve the scheduling of space to provide effective use.
- Design spaces to increase the perception of natural surveillance.
- Overcome distance and isolation through improved communications and design efficiencies, e.g., intercoms, emergency call stations, pedestrian paths and emergency (blue light) phones.
- Turn *soft* targets into *hard* targets.

98. ENVIRONMENTAL SECURITY

"Environmental security" is an urban planning and design process that integrates crime prevention with neighborhood design and urban development. It is a comprehensive environmental design approach that combines traditional techniques of crime prevention with newly developed theories and techniques. Environmental security is concerned with the reduction of not only crime but also the fear of crime, since it has become recognized that the fear of crime is equally serious and is a major contributor of the urban decay process.

The main idea behind Environmental Security is that our urban environments can be designed or redesigned to reduce criminal opportunities and the fear of crime. We need not resort to building fortresses that result in the deterioration in the quality of urban life.

Crime and the fear of crime are among the main reasons for reduced urban investment and flight to the suburbs. Every day, the newspapers and television remind us of the problems of uncontrolled street crimes where no individual is safe. Public opinion surveys consistently identify crime as one of the major problems confronting our cities and their urban neighborhoods.

99. THE NEIGHBORHOOD AND FEAR OF CRIME

To understand how geography relates to Neighborhood Watch programs, we must first understand why people's fear of crime matters. James Garofalo of the State University of New York at Albany defines fear as the emotional response to a sense of danger and anxiety about physical harm. Fear of crime, then, relates to the potential for such harm to be inflicted during a crime event.[13]

According to Garofalo, people tend to associate the threat of physical harm with certain places: where they live, a place they are visiting, somewhere they want to go, or a place they avoid. And although crime can happen anywhere, certain locations experience crime more frequently.[14] Generalizations about crime rates help establish

[13] Garofalo J. The fear of crime: causes and consequences. *Journal of Criminal Law and Criminology* 1981;**72**(2):839–57.

[14] Wolfgang M. *Patterns in criminal homicide*. University of Pennsylvania Press, Philadelphia, 1985; Sherman LW. Hot Spots of Crime and Criminal Careers of Places. In: Eck JE, Weisburd D, editors. *Crime and place*. Criminal Justice Press, Monsey, NY; 1995. p. 35–52.

the psychological link between the likelihood of a crime occurring in that place and a person's fear of being a crime victim.

CPTED[15] reduces crime and fear of crime. (see CPTED section) using:

- *Territoriality*: attitude of maintaining perceived boundaries. The outsider is recognized and observed.
- *Natural Surveillance*: ability of inhabitants of an area to casually and continually observe public areas.
- *Image and Milieu*: design to counteract the perception that the area is isolated and vulnerable to crime.
- *Safe Areas*: locales that allow for high degree of police observation.
- Incorporating urban planning with crime prevention.

Reduce crime through environmental security by:

- *Increasing Perpetration Time*: more difficult to commit the crime.
- *Decreasing Detection Time*: enhanced lighting, landscaping, etc.
- *Decreasing Reporting Time*: better observation by more people.
- *Decreasing Police Response Time*: better planning of streets, clearly marked exits and pathways.

In *Defensible Space*,[16] author Oscar Newman states that better residential security can be obtained through environmental and architectural design that is coordinated with crime prevention methods.

100. CRIME PREVENTION THROUGH INTEGRATED PROBLEM SOLVING: BROKEN WINDOWS

Have you ever conducted a risk assessment only to find that the property was the worst of the worst? The housing unit was gang infested with open selling of drugs on the sidewalk. Even the homeless were working for the drug dealers, and they were given cell phones to call when they saw the police.

The facilities office was at the front of the complex, and the cameras that worked were at the rear up on the third floor, unattended. This was a large complex of 240 units with two small dumpsters and trash everywhere on the grounds. Windows were boarded up; I originally thought they had several fires, but it was to prevent them from being broken into. Law Enforcement refused to respond without necessary backup. Truly a horror show.

George Kelling was one of the authors of *Broken Windows* (1982) along with James Q. Wilson; they have said "we must reduce disorder and you will reduce crime."

[15] Crowe TD, Fennelly LJ. *Crime prevention through environmental design*, 3rd ed. Elsevier, Boston, MA; 2013.
[16] http://www.defensiblespace.com.

The Former Commissioner of the New York Police William Bratton has said "The strategy is sending a strong message to those who committed minor crimes that they will be held responsible for their acts."

Suggested strategies:

Community partnerships formulated
Communication with Law Enforcement improved
Police coverage with K-9
Law enforcement as resident of complex
A police substation established
Tenants who are dealing become evicted
Lighting increased
Security surveillance system fixed
Security officers assigned
Neighborhood watch established
Control of public and private space taken back
CPTED security landscape implemented
Chronic issues addressed and not ignored

Source: Fixing Broken Windows, George L. Kelling & Catherine M. Coles, The Free Press, 1996, also 150 Things You Need to know About Physical Security, 2016, Elsevier.

101. PARKING LOTS AND GARAGES

Parking lots and parking garages must have natural surveillance and natural access control. Routes of travel for vehicles and pedestrians should be clearly identified and marked. Surveillance by both casual observers and law enforcement will help to create a surface parking lot or parking garage that "feels" safe to legitimate users. Proper landscaping design and principles can certainly make the difference toward creating an "open" parking garage or surface parking lot and a "closed" parking garage or surface parking lot. Parking lots or parking garages that have dark areas because there is not adequate lighting are considered "closed" environments that do not "feel" safe. They may have enclosed stairwells or tall bushes that have not been maintained, which create hiding places. Additionally, many times there is no security present, and this may cause users to "feel" unsafe and vulnerable.

Some of the concepts below apply to parking garages as well as surface parking lots:

- A well-distributed security surveillance system that monitors drive paths, parking spaces, elevator lobbies, and stairwells
- Emergency call buttons (blue light phones) for emergency assistance at vulnerable areas, especially in elevators and on each level of the parking structure
- Open and wide line of sight
- Clearly visible signage at all entrances and exits
- Open stairways with clear line of sight from the outside
- Regular patrols by uniformed security and law enforcement (or both) utilizing a guard tour system to document varying routes
- Limited entry points for pedestrians and vehicles
- Bright walls, ceilings, and colorful décor
- White walls and ceilings to enhance reflectivity
- Effective lighting that is properly maintained with upgrades to LED lights, which operate off a motion detector and will increase the level of light as you walk closer and under the fixture.
- According to lighting recommendations by the IESNA:
  - Covered parking structures and pedestrian entrances should be illuminated to 5.0 fc and garage elevators and stairs to 10.0 fc
  - An open parking lot should be illuminated to 0.20–0.90 fc
- Parking garages should have raised ceiling heights to enhance openness as well a signage that indicates the floor to ceiling height.
- Pedestrian entranceways designed with transparent glass to allow clear observation
- Directional signage indicating the locations of exits and/or elevators, and which floor you are on.

CPTED STRATEGIES

There are three overlapping strategies in CPTED:

1. Natural access control
2. Natural surveillance
3. Territorial reinforcement

Access control and surveillance have been the primary design concepts of physical design programs. At the outset of the CPTED program, access control and surveillance—preexisting as conspicuous concepts in the field of crime prevention through environmental design—received major attention. Access control and surveillance are not mutually exclusive classifications since certain strategies achieve both, and strategies in one classification typically are mutually supportive of the other. However, the operational thrust of each is distinctly different, and the differences must be recognized in performing analysis, research, design, implementation, and evaluation.

Natural access control is a design concept directed primarily at decreasing crime opportunity. Access control strategies are typically classified as organized (e.g., guards), mechanical (e.g., locks), and natural (e.g., spatial definition). The primary thrust of an access control strategy is to deny access to a crime target and to create a perception of risk in offenders. Surveillance is a design concept directed primarily at keeping intruders under observation? Therefore, the primary thrust of a surveillance strategy is to facilitate observation, although it may have the effect of an access control strategy by effectively keeping intruders out because of an increased perception of risk.

Surveillance strategies are typically classified as organized (e.g., police patrol), mechanical (e.g., lighting), and natural (e.g., windows).

These Typical Concepts and Strategies

Traditionally, access control and surveillance, as design concepts, have emphasized mechanical or organized crime prevention techniques while overlooking, minimizing, or ignoring attitudes, motivation, and use of the physical environment. More recent approaches to physical design of environments have shifted the emphasis to natural crime prevention techniques, attempting to use natural opportunities presented by the environment for crime prevention. This shift in emphasis led to the concept of territoriality.[17]

THE GROVE: A LOS ANGELES EXAMPLE[18]

When the company Caruso Affiliated was designing The Grove, an innovative shopping district near Los Angeles' old Farmers Market, they decided they wanted the "best parking garage in Los Angeles." They recognized the need for extensive redesign of their existing plans, and turned to CPTED to solve the traditional problems with garage design and construction. As a result, the garage turned out to be an exemplary design employing the following CPTED and conscientious operational components: (1) limited access points for pedestrians and cars; (2) bright walls, ceilings, and colorful décor; (3) exemplary lighting for its time, with halide luminaires; (4) raised ceiling heights; (5) very large and furnished elevator lobbies on each floor; (6) moderate but well-distributed camera system and callboxes; (7) very long and wide open sight lines; (8) traffic-oriented entries and exits; (9) open stairways; (10) regular security patrols.

Some municipalities do have design snippets (CCTV, lighting, security patrols), and the National Institute of Building Sciences posts a few as well. There are also a number of CPTED books that promote good parking lot design. However, CPTED practitioners must ensure these practices are implemented. As cities construct more covered parking in the 21st century, CPTED must play a significant role in assuring the safety and security in these potential vulnerable spaces.

---

[17] CPTED Perspective, Vol. 12 Issue Jan/Sept 2015 and NIJ, CPTED April, 1996, p. 10 updated Oct. 2016 Fennelly & Perry.

[18] ICA, CPTED Perspective, Jan/Sept 2015 newsletter issue 1.

PART

Fire Protection, Emergency Management, and Safety

4

102. FIRE PROTECTION AND SAFETY[1]

Greg Benson and Michael Fagel

Although the potential for all types of fires exists and should be planned for, certain production areas are more likely to experience a fire based on specific process or material. This condition should be considered when assigning extinguishers to the department or facility. Every operation is potentially subject to Class A (common combustibles) and C (energized electrical) fires, and most are also threatened by Class B (flammable liquid) fires to some degree.

Having made such a determination, professionals must then select the types of fire extinguishers most likely to be useful. The choice of extinguisher is not difficult, but it can only be made after the nature of the risks is determined. Extinguisher manufacturers can supply all pertinent data on the equipment they supply, but the types in general use should be known. It is important to know, for example, that over the past 20 years the soda/acid and carbon tetrachloride extinguishers have been prohibited and are in fact no longer manufactured. In addition, an extinguisher that must be inverted to be activated is no longer legal.

FIRE EXTINGUISHERS

After extinguishers have been installed, a regular annual program of inspection and maintenance must be established. A good policy is for safety/security personnel to check all devices visually once a month and to have the extinguisher service company inspect them at least annually twice a year. In this process, the serviceman should retag, and if necessary, recharge the extinguishers and replace defective equipment. Inspections and maintenance should be documented.

HIGH-QUALITY FIRE EXTINGUISHERS

Whether you need a new extinguisher, an inspection, or testing, we can replace parts for extinguishers from any manufacturer. You will have peace of mind knowing that you your family and your property are protected.

[1] http://www.gorhamfire.com/quincy-ma-fire-extinguishers.htm.

Physical Security: 150 Things You Should Know. http://dx.doi.org/10.1016/B978-0-12-809487-7.00004-8

Pressurized water models: appropriate for use on Class A fires only. These must never be used on electrical or flammable-liquid fires.

Carbon dioxide: extinguishers contain pressurized liquid carbon dioxide, which turns to a gas when expelled. These models are rated for use on Class B and C fires, but can be used on a Class A fire. Carbon dioxide does not leave a residue.

Dry chemical extinguishers: either stored-pressure models or cartridge-operated models. The stored-pressure models have a lever above the handle for operation. The cartridge-operated models require two steps: (1) depress the cartridge lever, and (2) then squeeze the nozzle at the end of the hose. The dry chemicals leave a residue that must be cleaned up after use.

Ammonium phosphate: dry chemical that can be used on Class A, B, and C fires, but should never be used on a fire in a commercial grease fryer because of the possibility of reflash and because it will render the fryer's automatic fire protection system less effective.

Sodium bicarbonate: dry chemical, suitable for fighting Class B and C fires; it is preferred over other dry chemical extinguishers for fighting grease fires. Where provided, always use the extinguishing system first. This also shuts off the heat to the appliance.

Potassium bicarbonate, urea-base potassium bicarbonate, and potassium chloride: dry chemicals are more effective and use less agent than sodium bicarbonate on the same fire.

Foam (or AFFF and FFFP) extinguishers: coats the surface of a burning flammable liquid with a chemical foam. When using a foam extinguisher, blanket the entire surface of the liquid to exclude the air.

Source: Fisher RJ, Green, G. *Introduction to Security*, 6th ed.: Butterworth-Heinemann; 1998. Updated and reviewed by Michael Fagel, Ph.D., CEM, and Fire Chief Greg Benson, CFO, CPSE, COOP, in April 2016, plus http://www.gorhamfire.com/quincy-ma-fire-extinguishers.htm.

103. NATIONAL FIRE PROTECTION ASSOCIATION

Greg Benson and Michael Fagel

We have always felt very strongly that law enforcement and security should work close with local fire departments. The National Fire Protection Association (NFPA) has a considerable amount of material available, if you should ever need it. Some standards with which you and your personnel department should be familiar are:

NFPA 1001	Standard for Firefighter Professional Qualifications
NFPA 1002	Standard for Fire Apparatus Driver/Operator Professional Qualifications
NFPA 1003	Standard for Airport Firefighter Professional Qualifications
NFPA 1004	Standard on Firefighter Medical Technicians Professional Qualifications
NFPA 1021	Standard for Fire officer professional Qualifications
NFPA 1031	Standard for Professional Qualifications for Fire Inspector, Fire Investigator and Fire Prevention Education Officer
NFPA 1041	Standard for Fire Service Instructor Professional Qualifications

NFPA 104–3.4.3	Extinguishing Recordkeeping (tags)
NFPA 13	Sprinkler Head Flow Rate
NFPA 17	Dry Chemical Extinguishing Systems
NFPA 12A	Halon Agent Extinguishing Systems, Blower Door Fan Unit

APPENDIX B

NFPA 10A-3.2	Extinguisher Size and Placement for Cooking Media
NFPA 25 6–3.1	Water Based Fire Protection Systems/Testing Procedures
NFPA 1221	Public Fire Alarm reporting System
NFPA 72	Protective Signaling Systems, Testing and Maintenance
NFPA 80	Fire Doors, Installation, Testing and Maintenance
NFPA 99	Standard for Health Care Facilities, 1999 Edition

Source: Schaub JL, CPP, Biery Jr KD. *The Ultimate Security Survey*: Butterworth-Heinemann; 1994, pp. 154–60. Updated and reviewed by Michael Fagel, Ph.D., CEM, and Fire Chief Greg Benson, CFO, CPSE, COOP, in April 2016, and NFPA Website www.nfpa.org. May 2016.

104. FIRE PROTECTION PROGRAMS (FPPs)

Factory Mutual Engineering and Research recommends three Fire Prevention Programs (FPPs), which are formulated to: monitor conditions to detect and correct deficiencies promptly and control and minimize or avert risks that can cause or contribute to fires.

Each of the three Fire Protection Programs:

Follow systematic, preplanned procedures.
Require regular, scheduled inspections.

FM Global understands the numerous challenges facing risk managers and companies and has designed products and services to support risk identification and assessment, risk avoidance and risk reduction, risk acceptance, and risk transfer. This comprehensive approach is fully integrated into their business model.

The three Fire Prevention Programs are as follows.

RISK IDENTIFICATION AND RISK ASSESSMENT

Consider regular on-site assessments combined with risk analysis expertise and provide an accurate assessment of the potential loss and its impact.

RISK AVOIDANCE AND RISK REDUCTION

Consider scientifically based solutions that go beyond insurance to impact the cost of risk equation, select the best options, execute them, and manage and maintain change.

RISK ACCEPTANCE AND TRANSFER

A clear assessment of the underlying risk will help determine whether to accept or transfer the risk. When transferring risk, your insurance company must be able to provide a capacity commitment with proven reliability.

105. FIRE INSPECTIONS

Greg Benson and Michael Fagel

Fire inspections not only prevent fires but also present opportunities to better evaluate and inspect your facility to ensure compliance with fire, building, and life safety codes. Fire inspections should be carefully and systematically planned and should emphasize fire prevention. Your plan should incorporate how you will prevent fires from starting and from spreading and how you will ensure compliance with the fire protection, building, and life safety codes.

Familiarize yourself with the local laws and administrative codes of your city. Many times, the inspection of your facility is predicated on its type of occupancy and building classification. Realize that local laws affect smoke-detecting devices, power sources, general requirements for smoke-detecting devices, and the inspection of these devices.

Outline how your inspections will be conducted, who will conduct them, what training levels required, and who will review what was inspected. Have members of your department conduct inspections on a daily, weekly, or monthly basis. Never underestimate the value and effectiveness of your inspections. Your municipality will be impressed when you specify the purpose of inspections and how you intend to conduct them.

If your facility uses a watch clock or electronic device for recording daily fireguard patrols, discuss this in this section. Keep a separate log book for fireguard patrols. In this log book, indicate the locations of all the stations, and the name, date, and time the employee made the watch clock tour. Upon employees' completion of their tours, they should sign the log book, indicating the time they began the tours and the time they completed the tours. A supervisor's signature should accompany each entry. This log book should be filed for 5 years. During an inspection by the fire department, it would behoove you to show them these records. Employees should look for the following items during inspections:

Adequate lighting in stairways and hallways
Operational emergency lighting
Accessibility of doors serving as means of egress
Availability and proper spacing of fire extinguishers
Usability of fire extinguishers

Posting of no smoking signs
Operational and properly placed exit signs
Rubbish accumulation or unsanitary conditions

Source: Cassidy K. *Fire and Safety & Loss Prevention*: Butterworth-Heinemann; 1992. Updated and reviewed by Michael Fagel, Ph.D., CEM, and Fire Chief Greg Benson, CFO, CPSE, COOP, in April 2016.

106. CLASSES OF FIRE[2]

Greg Benson and Michael Fagel

All fires are classified in one of four groups. It is important that these groups and their designations be widely known since the use of various kinds of extinguishers depends on the type of fire to be fought.

Class A: Fires of ordinary combustible materials, such as wastepaper, rags, drapes, and furniture. These fires are most effectively extinguished by water or water fog. It is important to cool the entire mass of burning material to below the ignition point to prevent rekindling.

Class B: Fires fueled by substances such as gasoline, grease, oil, or volatile fluids. The latter fluids are used in many ways and may be present in virtually any facility. Here a smothering effect such as carbon dioxide (CO_2) is used. A stream of water on such fires would simply serve to spread the substances, with disastrous results. Water fog, however, is excellent since it cools without spreading the fuel.

Class C: Fires in live electrical equipment such as transformers, generators, or electric motors. The extinguishing agent is nonconductive to avoid danger to the firefighter. Electrical power should be disconnected before beginning extinguishing efforts.

Class D: Fires involving certain combustible metals such as magnesium, sodium, and potassium. Dry powder is usually the most, and in some cases the only, effective extinguishing agent. Because these fires can only occur where such combustible metals are in use, they are fortunately rare.

Class K: Fires in cooking appliances that involve combustible cooking media (vegetable or animal oils and fats). During an emergency, the actual shutdown of equipment should be assigned to people familiar with the process.

Plan Ahead! If a fire breaks out in your home or office, you will have only a few minutes to get out safely once the smoke alarm sounds. Everyone needs to kno*w what to do and where to go if* there is a fire.

SMOKE DETECTORS

There are two types of smoke detectors: ionization and photoelectric. Each type has characteristics that enhance effectiveness.[3]

[2] *Effective physical security*, 5th ed. Elsevier, Cambridge, MA; 2017.
[3] Onization vs Photoelectric. (February 26, 2014). http://www.nfpa.org/safety-information/for-consumers/fire-and-safety-equipment/smoke-alarms/ionization-vs-photoelectric.

Ionization

Ionization-type alarms utilize a small amount of radioactive material between two charged plates. Air is ionized as it flows between the plates. Smoke entering the chamber disrupts the flow of ions causing the alarm to activate. Ionizing alarms are more responsive to flaming fires.

Photoelectric

Photoelectric detectors utilize a light source in the sensing area to detect the presence of smoke. Photoelectric detectors work better with smoldering fires.

Source: Fisher RJ, Green G. *Introduction to Security*, 6th ed.: Butterworth-Heinemann; 1998. Updated and reviewed by Michael Fagel, Ph.D., CEM, and Fire Chief Greg Benson, CFO, CPSE, COOP, in April 2016, and Effective Physical Security, Elsevier, fifth edition, 2017, Onization vs Photoelectric. (February 26, 2014). http://www.nfpa.org/safety-information/for-consumers/fire-and-safety-equipment/smoke-alarms/ionization-vs-photoelectric.

107. FIRE PREVENTION AND SUPPRESSION: A CHECKLIST

Is there a comprehensive written plan addressing fire prevention and suppression policies, training levels, techniques, and equipment disseminated to all employees?

Are fire drills conducted on a regular basis (at least once every six months)?

Have individuals been assigned specific responsibilities in case of fire?

Is smoke/fire detection equipment installed in the computer area?

Does the smoke/fire detection system in the computer area automatically:

- Shut down or reverse the ventilation air flow?
- Shut down power to the computer system?
- Shut down computer area heating?

Is the computer area smoke/fire detection system serviced and tested on a regularly scheduled basis?

What devices are incorporated into the computer area smoke/fire detection system'?

- Ionization smoke detectors?
- Photoelectric smoke detectors?
- Heat rise detectors?
- Others (specify)?

Specify how many of these components are located in the computer area and where they are placed?

Is there equipment available in the computer area to exhaust smoke and combustion products directly to the atmosphere after a fire?

Are smoke detectors placed and functioning properly in the computer area (in the ceiling, under the raised floor, and in all high vacuum air conditioner (HVAC) ducts)?

How often are these smoke detectors tested? By whom?

Will the smoke detectors operate in a power failure situation?
Is an automatic sprinkler system installed to protect against fires in the computer area open space?

108. SMOKE ALARMS: AS EASY AS 1–2–3

CHOOSING

There are two types of power to smoke alarms: battery operated and hard wired into electrical control panel with battery back up.

The hard wired alarm has the advantage of using a backup power if the AC power fails. These are considered more reliable in the long term. In the next 5 years, it is expected that this technology will change.

Alarm horns and/or voice communication speakers are usually located next to every stairwell door on all floors.

INSTALLATION

If you can handle a screwdriver, you can install a battery-operated smoke alarm. They are simply fastened with two small screws. Hard-wired smoke alarms must be installed by a licensed electrician.

HOW MANY DO YOU NEED?

A smoke alarm outside each sleeping area with a minimum of one on each level provides a reasonable degree of protection from the threat of fire.

A passageway or corridor between the living areas and the bedroom is an ideal location. Homes with separate sleeping areas need extra alarms.

Where occupants tend to sleep with bedroom doors closed, a smoke alarm should be installed in each bedroom, particularly if heaters or electrical appliances are used in those rooms.

Local ordinances or regulations should be used in determining the number and placement of smoke detectors.

WHERE IS THE BEST POSITION?

Smoke alarms should be positioned on flat ceilings away from dead corners, exposed beams, or any other fixture that may deflect smoke.

If installed on a wall, the top of the smoke alarm should be located 100–300 mm from the ceiling.

TREND

A new law in New York mandates that smoke detectors must now contain nonremovable batteries with a working life of 10 years. This was signed into law on January 4, 2016, going into effect January 1, 2017.

109. SMOKE ALARM SYSTEMS: A CHECKLIST

Is all equipment currently in place underwriters lab listed?
Is the equipment using all state-of-the-art technology and working?
Is the alarm system equipped with audible signals, bells, sirens, voices, and/or strobe lights and does it sound locally?
Does the complex own its alarm system?
If not, is a leased alarm system agreement in effect?
Which alarm leasing company is used?
Does the lease include a maintenance and service contract?
Is an off-site central station used to monitor the facility's alarm system?
Is the alarm system monitored by direct connection to a central monitoring facility?
Is the monitoring of the alarm system proprietary (in-house)?
How frequently is the system completely tested?
How frequently does the system have false alarms?
Is the overall authorized response time adequate?

MAINTENANCE

Smoke alarms should be tested and cleaned periodically. Semiannually is recommended. Smoke alarms have a test button. This should be pressed (using a broom handle or similar rod) at least once every month to prove that the alarm will sound.

At least once a year the fine nozzle of a vacuum cleaner or a soft brush should be run over the grille area of each smoke alarm.

In most models when batteries are low the alarm will regularly sound a short "beep." This is a reminder to replace the batteries. Once a year batteries should be replaced, e.g., New Year's Day, birthdays (that would also be a good time to clean the grille). Smoke alarms must never be painted.

WHY EVERYONE SHOULD HAVE A SMOKE ALARM

When there is a fire in a house, the house fills with toxic smoke and gases long before heat and flame can spread.
Most people who die in fires are killed by toxic smoke. Many are never touched by flames.
Most people who die in fires die at night because they are asleep.
A smoke alarm is your safeguard against this danger because it detects the presence of smoke at a very early stage and sounds an alarm.
A smoke alarm gives you the warning to escape before the smoke has made it too difficult.
The NFPA has found that working smoke detectors reduce the risk of fatalities in a house fire by 50%.

Almost two-thirds of the fatalities occur in homes in which a smoke detector is not present or not operational due to lack of maintenance.
(NFPA Fast Facts About Smoke Alarms)

110. MAINTENANCE OF FIRE PROTECTION EQUIPMENT

Equipment	Typical Maintenance	Why	Frequency
Hydrants	Inspect and lubricate	To ensure it is operational and that caps and valve can be easily operated	Annually
Pumper and standpipe connection	Flush (hydrants)	To ensure lines are clear of debris	Annually
Check valves/ alarm check valves	Inspect and clean	To ensure clapper moves freely and that gasket is in good condition to prevent leakage	Every 5 years
Control valves (PIV, PIVs, OS&Ys, IBVs, etc.)	Fully close and reopen (courting turns), lubricate	To ensure that valve is operable	Annually
Dry pipe valves, preaction valves, deluge valves	Trip test, inspect and clean	To ensure valve is operational, clapper moves freely and gasket is in good condition	Annually
Dry system	Flushing investigation	To ensure that piping is free of scale and other obstruction	Every 15 years, then every 5 years
Fire pumps	Test starts automatically	Ensure that pump and controller is operational in the automatic mode	

111. REDUCING FALSE ALARMS

FALSE ALARMS

To avoid nuisance alarms, standard alarms should not be installed in kitchens or in positions where the normal airflow is through an area where smoke or fumes are generated. Some models allow you to temporarily silence alarms caused by smoke from cooking or smoking. In any case, the alarm will stop sounding as soon as the smoke has cleared.

Ninety-five percent of the time, dirt is the main cause of false alarms. Either that, or the battery is dying. Set a policy for the replacement of all batteries to be replaced at the same time, to prevent false alarms and save on cost.

FIRE ALARMS

Smoke detectors: Solution is to check dirty heads or smoke detectors installed near a dusty product or laundry room. The proper type of smoke detector for the area will reduce the number of false alarms. They should be cleaned twice a year to prevent false alarms.

1. Equipment malfunction. Solution is annual maintenance.
2. Failure to properly tag circuit breakers.

The key here is maintenance. The systems are not that complex. Effective physical security concepts are still:

1. People and training.
2. Procedures and enforcement.
3. Hardware-reliable and effective.
4. Facilities security function.
5. Information reporting and proactive response.

112. TEN QUALITIES OF A WELL-PROTECTED FACILITY

The following are the 10 basic human elements and physical protection qualities of a well-protected facility.

MOTIVATED MANAGEMENT AND STAFF

Genuine interest in good loss prevention by management and employees is *the most important component* of an effective loss control program. It is management's responsibility to:

Implement a Safety/Security Committee with representation from all levels of the organization.
Establish Safety/Security Committee program goals.
Properly fund the Safety/Security program.
Develop and implement comprehensive written program policies.
Deliver training to meet program goals.
Provide state-of-the-art equipment.
Offer incentives.
Regularly evaluate Safety/Security programs and update as needed.
A culture that recognizes and embraces safety and security will provide long-term sustainable programs.

CONSTRUCTION SUITABLE FOR OCCUPANCY

Special consideration should be given to occupancies (processes, hazards, and equipment), which are especially:

Hazardous (highly combustible or explosive; flammable liquids, explosive dusts, etc.).
High value and especially sensitive to fire-related damage (computers, switching equipment, etc.).
Critical infrastructure for the community, region, or nation.

AUTOMATIC SPRINKLERS

Automatic sprinklers have been proved to be the most cost-effective and reliable form of protection. Local fire prevention and building codes will provide specific guidance and requirements on built-in fire protection systems.

In general, automatic sprinklers are recommended for:

any facility of combustible construction
any facility containing a significant amount of combustibles
enclosed or adjoining equipment or spaces in which fire can start and spread.

The Authority Having Jurisdiction (AHJ) should be contacted regarding fire protection requirements. The Fire Code adopted by the AHJ will determine specific protection system requirements. All fire protection systems should be designed and installed by qualified, licensed contractors.

SPECIAL HAZARDS

Special processes and materials such as flammable liquids, combustible gases and dusts, plastics, and rubber tires, may require specific fire protection needs. Other challenging situations include handling, storage height, storage arrangement, location, and access. Areas with information technology (IT) equipment may require specialized protection systems.

WATER SUPPLY ADEQUATE FOR CHALLENGE PRESENTED BY OCCUPANCY

For automatic sprinklers to operate effectively, water volume and pressure must be sufficient for challenge presented by building and occupancy. Changes in building use or occupancy may require revision to fire protection system for code compliance.

An improperly closed valve (lCV) can allow an otherwise controllable fire to grow into a catastrophe. Four procedures can help prevent lCVs:

Lock all valves open
Regularly inspect all valves
Use Shut Valve Tag Procedures to track valves that have been closed for repairs
Install alarm system monitoring capability on valves.

ADEQUATE MAINTENANCE OF BUILDINGS AND EQUIPMENT

Problems with either building or equipment can result in business interruption, economic loss, and reduction in employment. Effective maintenance requires scheduled inspections, preventive maintenance, and expedient repairs.

GOOD HOUSEKEEPING

This is required to prevent:

Fire spread through combustibles, which should not be present.
Blocked access to valves, hoses, and extinguishers.
Blocked exits.

It can be implemented through:

Regular inspections that are scheduled and documented.
Training.
Employee awareness.

EFFECTIVE EMERGENCY ORGANIZATION

An effective Emergency Organization:

Works in conjunction with physical protection systems to minimize loss.
Requires careful planning and thorough assessment of emergency needs.
Is fully staffed with personnel who are trained, equipped, and prepared to respond to an emergency.
Focuses on prevention, preparation, response, and recovery from incidents.

PROTECTION AGAINST SERIOUS EXPOSURE FROM NEIGHBORS AND THE ELEMENTS

Preplan to minimize or prevent loss caused by:

Hazards in neighboring operations.
The effects of severe weather on buildings and yard equipment.

Source: Arkwright Factory Mutual System, www.factorymutural.com. Updated and reviewed by Michael Fagel, Ph.D., CEM, and Fire Chief Greg Benson, CFO, CPSE, COOP, in April 2016.

113. COMPUTERS: FIRE PROTECTION

Buildings housing computer centers should be of made of noncombustible construction materials to reduce the chance of fire. These facilities must be continuously

monitored for temperature, humidity, water leakage, smoke, and fire. Most building codes today require that sprinkler systems be installed.

Remember that water and electrical equipment do not mix. It is preferable to install a dry pipe sprinkler rather than a wet pipe system. Dry pipe systems only allow water into the pipes after heat is sensed. This avoids potential wet pipe problems, such as leakage. In addition, fast-acting sensors can be installed to shut down electricity before water sprinklers are activated. Sprinkler heads should be individually activated to avoid widespread water damage.

Another type of fire-suppression system uses chemicals instead of water. The two approved types of chemical were Halon 1301 and Halon 1211. Halon systems are still in common use, but the chemical itself was banned in 1994 by the United Nations because it contributes to destruction of the ozone layer in the upper atmosphere. Once this system is utilized, it must be recharged with either recycled Halon or the fire-suppression system must be slightly modified and FM-200 installed. FM-200 is similar to Halon, but with no atmospheric ozone-depleting potential. Carbon dioxide flooding systems are also available, but should never be used. Carbon dioxide suffocates fire by removing the oxygen from the room. Although this effectively extinguishes most fires, it also suffocates people still in the affected area.

All chemical fire suppression systems are relatively expensive and require long and complex governmental approval to install. Chemical fire suppression systems neither protects people from smoke inhalation nor can they deal effectively with electrical fires. They are, however, the only fire suppression systems that do not require computer equipment to be turned off, assuring the quickest possible return to normal operations.

There should be at least one 10-pound fire extinguisher within 50 feet of every equipment cabinet. At least one 5-pound fire extinguisher should also be installed for people unable to handle the larger units. These extinguishers should be filled with either PHalon, FM-200, or carbon dioxide. None of these agents requires special cleanup.

Install at least one water-filled pump-type fire extinguisher to use for extinguishing minor paper fires. Employees should be trained and constantly reminded not to use water extinguishers on electrical equipment because of the possibility of electric shock to personnel and damage to the equipment. They should also be discouraged from using foam, dry chemical, acid water, or soda water extinguishers. The first two are hard to remove and the others are caustic and will damage computer components.

Source: Fisher RJ, Green G. *Introduction to Security*, 6th ed.: Butterworth-Heinemann; 1998. Updated and reviewed by Michael Fagel, Ph.D., CEM, and Fire Chief Greg Benson, CFO, CPSE, COOP, in April 2016.

114. EMERGENCY PLANNING

Develop an effective and comprehensive, Emergency Response Plan. Provide training and education for the faculty and staff.

Comply with *all* applicable state and local codes.

Establish emergency procedures with standardized actions and directives for inclement weather (tornado, earthquake, hurricane, flooding, etc.), medical issues, fire, building evacuations, shelter-in-place, lock-down, workplace violence, and active shooter, as well as a business continuity plan for after the incident (OSHA, NFPA, FEMA, etc.).
Ensure your emergency procedures comply with Americans with Disabilities Act (ADA) Standards (physically handicapped, visually impaired, hearing impaired, special needs students, faculty, staff and visitors, etc.). Have designated individuals trained to assist.
Conduct regular training and joint exercises for emergency procedures with the local FD, PD, and EMS and other local officials. Provide floor plans for each building on the campus to each of these departments. Consider supplying building plans and layout of campus in a digital format on thumb drives for quicker access by more responders. Update the thumb drives that can be issued to teams on a quarterly basis. The main servers may be down, as well as cloud-based, so a thumb drive for a laptop may be the only available tool (install thumb drives in exterior locked Knox or Supra Boxes).
Establish a Crisis Management Team with documentation, training and integration into the larger Incident Command Team.
Determine who has the immediate authority to lock down and issue alerts and talk to the press. Establish a Joint Information Center with an appropriately trained public information officer who can supply vetted information that comes from the command staff only.
The Crisis Management Team will integrate into the response and recovery operations and will work closely with the first responder community as the situation ebbs and flows.
Develop procedures for during and after a crisis situation.
Develop Mass Notification Procedures (see Mass Notification).
Provide two-way radio batteries, chargers, cases, and training (or another alternative method for communication) for faculty and staff and establish a designated command center area or location.
The staff should follow the prescribed plan and report to the Emergency Command Center, (ECC) or other predesignated area for response and recovery. This may not be at the same site due to safety reasons and may be at a remote location.
Administrators will need to be at different locations and not in the immediate area of the event for their own and response operations safety.
Ensure you are in compliance with all applicable Occupational Safety and Health Administration (OSHA) regulations, Life Safety Codes, and local/state fire codes. NFPA 1600 is a useful tool to help comply with for all risks and all hazards planning.
Provide FEMA training for administration and crisis team members (http://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=is-100.sca).
Conduct fire, evacuation, lockdown, shelter-in-place, etc., drills.

Consider using the standard response protocol, "I love u guy's foundation."
Develop crisis kits with all necessary supplies for an emergency situation.
Develop GO BAGS for action teams.
Establish markings, vests, hats, or other easy identifications so that the school teams can be effectively identified to appropriate response officials.
Develop an effective and practiced mutual aid agreement with other organizations and businesses.
Collaborate with local law enforcement and all emergency response officials to establish protocols for shades and green cards to determine if interior door windows are to be covered and/or if shades are to be left open or pulled down in a lockdown situation.[4]

Source: Michael Fagel, Ph.D., CEM. Best Practices for Educational Environments: A 16 Point Master Plan, By Lawrence J. Fennelly, CPOI, CSSI, CHS-lll, CSSP-I & Marianna Perry, M.S., CPP, CSSP-I updated 2016.

115. WHAT MANAGERS NEED TO KNOW

When we say managers we are referring to:

- Local, state, and federal law enforcement
- Local, state, and federal government officials
- Hospital, school, and university public safety departments
- Security directors and security account managers
- Emergency managers
- Emergency responders
- Hospital board members
- School principals
- School board members
- Local education committees
- College and university leaders
- Campus groups and associations
- Risk managers and IT managers
- Facilities managers
- Nursing managers
- Hospital and campus safety stakeholders
- Managers of retail stores and malls
- Leaders of faith-based organizations
- Theater, sporting event, and concert managers

[4] Michael Fagel, Ph.D., CEM White Paper & Best Practices for Educational Environments: A 16 Point Master Plan by Lawrence J. Fennelly, CPOI, CSSI, CHS-lll, CSSP-I & Marianna A. Perry, M.S., CPP, CSSP-I.

In civil litigation, expert witnesses testify as to whether or not an act was foreseeable. One element of foreseeability is whether or not the area or the property had prior criminal activity. In many cases, the answer is, "yes," and therefore, the owner or manager of the property is put on notice that it is likely that additional crimes may occur in the future and action must be taken to mitigate the risks and keep people safe. This same premise can be applied to soft targets. Is the area vulnerable or "at risk" because of prior criminal activity or crime trends or is there an increase in a particular type of crime that has occurred in similar environments? Examples of soft target locations include:

- Colleges and universities
- Schools, K to 12
- Retail outlets and shopping malls
- Hospitals
- Hotels and motels
- Casinos
- Restaurants
- Sporting events
- Theaters and concerts
- Houses of worship

SEVEN THINGS YOU NEED TO KNOW ABOUT SOFT TARGETS

1. Never say, "It can't or will never happen here."
2. The Sandy Hook School shooting was over in about 6 min and 26 people were killed.
3. Perceived injustices and stereotypes have a powerful effect on the psyche of individuals. For example, the families of the nine people who were killed at an AME Church in Charleston, South Carolina, in June 2015, publicly stated that they forgave the shooter, Dylann Roof, when he appeared in court.
4. Shooters plan and assess their modes of action (the act) and escape. In the case of the shooting in the AME Church, the shooter was at the church for an hour (supposedly praying) before he opened fired on the community. When he was captured, the shooter, Dylann Roof, said, "I almost backed out because everyone was so nice at the Church."
5. Soft target hardening 101: is it possible to harden your target? In some cases, the perpetrators have been insiders or have had help from insiders. In her book, *Soft Target Hardening*, Dr. Jennifer Hesterman asks the question, "What is the cost of not protecting our people?"
6. Consider these six points as you develop your defense:
   a. The terrorist will first select or identify a vulnerable soft target.
   b. The terrorist will determine the method of attack.
   c. They will conduct detailed surveillance of the target to measure security forces.

d. They will assess target vulnerability and select the site or move on to another.
e. After site selection, a second round of surveillance will be conducted.
f. Finally, the operation will be scheduled and the attack conducted.

Do not encourage criminal activity or a terrorist attack by becoming a soft target. The most effective way to avoid indicating that you are a soft target is to remain at a high level of situational awareness. The sad truth today is that walking down a street on the way to a ball game in a downtown setting may place you in the middle of a battleground in a split second.

Your ability to recognize and perceive potential threats while going about routine activities will make the difference. Do not deny your gut feelings. As we all know, many good arrests made by law enforcement on the streets come from a gut feeling or intuition and then most importantly, acting upon that feeling or suspicion. "Situational awareness and the apparent readiness of that person indicate whether or not they are a hard target or soft target is crucial," states Sgt. Glenn French, a 22-year-old veteran with the Sterling Heights (Mich.) Police Department.[5]

7. The Six-Step, NIPP Risk Management Framework of the Commercial Facilities (CF) Sector provides an excellent starting point to protect your assets. We have included the Homeland Security Guidance below:[6]

SET GOALS AND OBJECTIVES

The Commercial Facilities Sector-Specific Plan (CFSSA) uses sector goals that define specific outcomes, conditions, end points, or performance targets as guiding principles to collectively constitute an effective risk management posture.

IDENTIFY ASSETS, SYSTEMS, AND NETWORKS

The identification of assets and facilities is necessary to develop an inventory of assets that can be analyzed further with regard to criticality and national significance. Because of the diverse nature of assets within the CF Sector, the CFSSA works with the DHS Infrastructure Information Collection Division (IICD) to identify and validate these assets. In addition to its collaboration with the IICD, the sector also identifies assets through interaction with trade associations and corporate owners and operators.

ASSESS RISKS

The CF sector approaches risk by evaluating consequence, vulnerability, and threat information with regard to a terrorist attack or other hazard to produce a comprehensive, systematic, and rational assessment.

[5] www.policeone.com/law-enforcement-news-06-30-15.
[6] www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf.

PRIORITIZE

The CF Sector Coordinating Council and the CFSSA have found that it is not appropriate to develop a single, overarching prioritized list of assets for the CF Sector. Instead, assets are categorized by using a consequence methodology that allows the CF SSA to drive sector-wide protection efforts.

IMPLEMENT PROGRAMS

Given the size and diversity of the CF Sector, there is no universal solution for implementing protective security measures. The owners and operators of CF Sector facilities implement the most effective protective programs based on their own assessments. Protective programs address the physical, cyber, and human dimensions.

MEASURE PROGRESS

The CFSSA has developed relationships with both public and private sector partners, including trade associations, corporate entities, and industry subject matter experts. Information sharing through these partnerships is used to assist in measuring progress through the creation of sector metrics. By measuring the effectiveness of protective programs and their actions, the CF Sector can continually improve the infrastructure at the facility and subsector levels.

FACILITY MANAGER RESPONSIBILITIES

As part of the Emergency Response Plan, your facility managers should:

- Implement and understand site security procedures.
- Institute security access controls (e.g., keys, security system pass codes).
  - Key fobs, door codes.
- Distribute critical items to appropriate managers/employees, including:
  - Pocket-sized floor plans in break-glass cabinets.
  - Keys and other access control measures
  - Facility personnel lists and mobile telephone numbers.
  - Daily schedules.
- Assemble crisis kits containing:
  - Radios tested and rotated batteries and chemical light sticks.
  - Floor plans.
  - Employee roster and emergency contact numbers.
  - Appropriate first aid kits.
  - Flashlights.
- Activate the emergency notification system when an emergency situation occurs, as well as a backup plan.
- Ensure that the facility has at least two evacuation routes.
- Coordinate with the facility security department to ensure the physical security of the location, as well as the alternate routes.

- Advise, according to plans and protocols, and if in higher education, timely Clery notification.
- Secure doors.
- Order area supervisors to immediately direct all personnel (employees, customers, visitors, vendors, etc.) in their area to evacuate the facility if it can be done safely and with caution.
- If an evacuation is not possible, go to the nearest restroom. Lock the door, turn off the lights. Follow protocols.
- Keep personnel as calm as possible and try to notify 911 (using cell phones or telephones) of your location, the number of occupants, and their status. Turn all cell phones to silent!
- Remain in the room until an appropriate all-clear signal is given or law enforcement arrives.
- Prepare an incident report documenting personal observations.
- Post evacuation routes in conspicuous locations throughout the facility.
- Place up-to-date and secure removable floor plans near entrances and exits for emergency responders.
- Include local law enforcement and first responders during training exercises.
- The training must be as realistic as possible.
- Encourage law enforcement, emergency responders, SWA teams, canine teams. and bomb squads to train for an active shooter scenario at their locations.
- Foster a respectful workplace.
- Beware of early indications of potential workplace violence and follow appropriate protocols as trained for the specific situation.[7]

The shootings at the Inland Regional Center in San Bernardino, CA, on December 2, 2015, by Syed Rizwan Farook and Tashfeen Malik in which 14 were killed and 22 were injured will certainly raise concerns about hiring practices and the relationships between employer, employee, and coworkers.[8]

We have conducted research on this topic because we are frequently asked the question, "Do you think these incidents are going to increase or decrease in frequency?" As we hear about more and more incidents nationwide, it does appear as though they are becoming more frequent.

A STUDY OF ACTIVE SHOOTER INCIDENTS IN THE UNITED STATES BETWEEN 2000 AND 2013

> *"The findings establish an increasing frequency of incidents annually. During the first 7 years included in the study, an average of 6.4 incidents occurred annually. In the last 7 years of the study, that average increased to 16.4 incidents annually. This trend reinforces the need to remain vigilant regarding prevention efforts and for law enforcement to aggressively train to better respond to—and help communities recover from—active shooter incidents."*

[7] Fagel M. *Active Shooter*. ASIS International Publishers, Virginia; 2015.
[8] http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-shooting-live-updates-htmlstory.html.

"The findings also reflect the damage that can occur in a matter of minutes. In 64 incidents where the duration of the incident could be ascertained, 44 (69.0%) of 64 incidents ended in 5 min or less, with 23 ending in 2 min or less. Even when law enforcement was present or able to respond within minutes, civilians often had to make life and death decisions, and, therefore, should be engaged in training and discussions on decisions they may face."[9]

Source: www.policeone.com/law-enforcement-news-06-30-15, www.dhs.gov/xlibrary/assets/nipp-ssp-commercial-facilities-2010.pdf, Fagel, Michael. Active Shooter, VA: ASIS International Publishers, 2015; http://www.latimes.com/local/lanow/la-me-ln-san-bernardino-shooting-live-updates-htmlstory.html, http://www.fbi.gov/news/stories/2014/september/fbi-releases-study-on-active-shooter-incidents/pdfs/a-study-of-active-shooter-incidents-in-the-u.s.-between-2000-and-2013, Updated and reviewed by Michael Fagel, Ph.D., CEM, and Fire Chief Greg Benson, CFO, CPSE, COOP, in April 2016.

116. TEN POINTS ON EMERGENCY MANAGER RESPONSIBILITIES

1. The jurisdiction's emergency manager oversees day-to-day emergency management programs and activities. The emergency manager works with elected and appointed officials to establish unified objectives regarding the jurisdiction's emergency plans and activities. This role entails coordinating and integrating all elements of the community. The emergency manager coordinates the local emergency with the NIMS.
2. Coordinating the functions of local agencies.
3. Coordinating the development of plans and working cooperatively with other local agencies, community organizations, private sector entities, and nongovernmental organizations.
4. Developing and maintaining mutual aid and assistance agreements.
5. Coordinating resource requests during an incident through the management of an emergency operations center.
6. Coordinating damage assessments during an incident.
7. Advising and informing local officials and the public about emergency management activities during an incident.
8. Developing and executing accessible public awareness and education programs.
9. Conducting exercises to test plans and systems and obtain lessons learned.
10. Coordinating integration of the rights of individuals with disabilities, individuals from racially and ethnically diverse backgrounds, and others with access and functional needs into emergency planning and response.

[9] http://www.fbi.gov/news/stories/2014/september/fbi-releases-study-on-active-shooter-incidents/pdfs/a-study-of-active-shooter-incidents-in-the-u.s.-between-2000-and-2013.

Source: Updated and reviewed by Michael Fagel, Ph.D., CEM, and Fire Chief Greg Benson, CFO, CPSE, COOP, in April 2016.

117. NATIONAL RESPONSE FRAMEWORK: FIVE MISSION AREAS[10]

The National Response Framework is an essential component of the National Preparedness System mandated in Presidential Policy Directive (PPD) 8:

National preparedness: PPD-8 is aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the nation.[11]

Prevention: The capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. As defined by PPD-8, the term "prevention" refers to preventing imminent threats.

Protection: The capabilities necessary to secure the homeland against acts of terrorism and man-made or natural disasters.

Mitigation: The capabilities necessary to reduce loss of life and property by lessening the impact of disasters.

Response: The capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.

Recovery: The capabilities necessary to assist communities affected by an incident to recover effectively.

TEN THINGS YOU NEED TO KNOW TO GET STARTED

Have an overall Vulnerability and Risk Assessment conducted. This assessment will become an asset to management, and it will give them different perspectives in which to see their property. Consider the following scenario:

What if you had too much hazardous material stored on-site and because it had always been that way, you did not realize that your existing protection and protective measures were inadequate?

1. We recently conducted a security assessment for over 25 residential buildings in the northeast, and we had a fairly large checklist when it came to emergency procedures. The conversation with management went something like this, "Do you have emergency procedures?" "Oh yes we do," was the reply. "Can we see them?" we asked. Their reply was, "…uh, mmm," or "It's here someplace." Our next question was, "Have you read them?" The answer was, "No, not yet." As assessors and trainers, we go over every section of the emergency plan with managers to make sure everyone is on the same page and then have them "sign off" that the emergency procedures program was totally reviewed and that they understand their roles and responsibilities.

[10] www.fema.gov/national-response-framework.
[11] Ibid.

2. Let us take that same example again—25 sites and 25 different managers, all of which are located in high crime areas. All of the sites have issues with drugs, gangs, and prostitution—within the tenant base of the buildings. Homeless individuals "live" on the properties and around all buildings. There are daily problems with safety issues and environmental factors. To make matters worse, the local fire department and police department do not want to respond to calls for service to the property because it is not safe. Normally, owners and/or managers would be most concerned about fire, severe weather, etc., that could cause physical damage to the property. Since this location is in an area not patrolled by law enforcement and not serviced by the fire department, it makes it more difficult to plan for emergency situations. It is not impossible, but much more difficult to plan ahead.
3. Managers need to get ahead of the curve before a crisis occurs and be more proactive. Business recovery and resumption are part of the responsibilities of owners and/or managers for business continuity. When there is a crisis, how people (tenants, employees, and visitors) will be protected during emergencies and disasters needs to be part of the plan. Life safety issues are the first priority and need to be addressed during the planning stage.
4. Some examples of the basic types of hazards a plan needs to address to protect assets are:
   Medical emergencies
   Active shooters
   Bomb threats
   Fires
   Chemical, biological, radiological, or nuclear incident
   Family/domestic violence
   Workplace violence
   Severe weather
   Environmental emergencies
   Building collapse
   Loss of power
   The unexpected—an airplane or UAV falls out of the sky in the middle of your property.

FEMA states that, "While 'prevention' may be a common term, it has specific meaning in the context of the Framework and the National Preparedness Goal. The Prevention Framework covers the capabilities necessary to avoid, prevent or stop a threatened or actual act of terrorism."[12] We call it being *proactive*.

ELEMENTS OF AN EMERGENCY CONTINGENCY PLAN FOR A SITE EMERGENCY

Have a working knowledge of OSHA and Fire Safety Code requirements.

[12] www.fema.gov/national-prevention-framework.

Train and educate employees/managers about their role during an emergency as well as the response to victims during evacuation and how assistance to people with special needs will be provided. During training, familiarize everyone with evacuation routes.
Ensure there are redundant modes of communication. Do cell phones and radios work on your property? Its better to find out now (during an assessment) rather than during an emergency situation.
You must have a notification plan in place with updated phone numbers that need to be called when there is an emergency.
There is a decision process for determining what is needed to address short- and long-term issues. Determine the best method to contain the problem.
A management analysis will be disseminated with the overall contingency plan.
The objective is full recovery

Times have changed. We need to be in a proactive, not reactive mode. In January 2015, 12 people were killed during a terrorist act in Paris, at the office of a satirical magazine. In June 2015, nine people were killed in a Wednesday evening prayer service in South Carolina. Also in June 2015, a small plane crashed into a home in Massachusetts. In all these instances, law enforcement, the fire department, and emergency medical personnel responded, along with the media. Every individual at every scene was attempting to provide assistance to the victims and also searching for answers as to how the situation occurred. The Boston Marathon incident when two pressure cooker bombs exploded happened even though numerous police officers and emergency personnel were on-site and video surveillance was being used.

The three P's of emergency planning:
- Planning
- Preparation
- Practice

An Emergency Support Function[13] is activated in response to an incident of national significance. All support agencies respond to meet operational needs and to participate in planning for short- and long-term incidences and recovery. The responding agencies also provide information and/or intelligence to law enforcement.
A Mutual Aid Agreement[14] is voluntary cooperation between industrial, business, and local government emergency services agencies whereby each agrees to assist one another during a disaster or emergency situation. It is important to communicate, coordinate, and verify all provisions of the emergency response and agreement. Disasters may be man-made, such as an active shooter, or a natural disaster, such as an earthquake. Business Continuity Planning is ensuring that essential business functions, processes, and procedures continue to operate

[13] www.fema.gov/pdf/emergency/nrf/nrf-esf-intro.pdf.
[14] www.usfa.fema.gov/pdf/efop/efo36537.pdf.

during and after a disaster. This planning enables the business or organization to reestablish services to a fully functional level as quickly and smoothly as possible. Business continuity planning will give businesses and organizations their best chance of surviving a disaster or emergency situation. Disaster recovery is how the business or organization resumes operations after a disaster or emergency situation.

How physical security helps:

Access control will keep sensitive areas locked and secured.

Vehicular access control will create established stand-off distances. For example, vehicles may be kept 50 feet from your building to secure the area.

A Security Surveillance System [closed-circuit televisions (CCTV)] can help serve as a buffer zone and aid in providing feedback to law enforcement as well as monitoring closely all utility openings/HVAC air intakes and the perimeter of the property.

Install adequate lighting on your property—especially by walkways, around doorways, and in parking areas. A properly illuminated area acts as a psychological and physical deterrent and can reduce criminal opportunity as well as aiding in your overall emergency operation.

How security officers can help

Crowd Control.

Closing access points; implementing additional security measures for high-profile areas and high-profile managers.

Training for what to do in an emergency situation.

Interface with law enforcement.

Provide protection to property. Security officers have the capabilities necessary to secure property against acts of terrorism and man-made or natural disasters.

Provide appropriate response. Security officers have the capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred.

In recent years, several lists of "Best Practices" have been developed by different groups in the security industry. We have been in the forefront of this movement with the formulation of "Best Practices of 2015." This is an adaptable document that can be applied to various circumstances to make it applicable for different environments.

Source: www.fema.gov/national-response-framework.

118. MUTUAL AID ASSOCIATIONS

A cooperative, voluntary organization of industries, businesses, and local government emergency services that have entered into a voluntary agreement to assist each other by providing materials, equipment, and personnel for disaster control during emergency situations. Community resources are identified and standardized equipment and training are provided.

The purpose is to establish a workable emergency management organization that minimizes damages and ensures early restoration or business continuity.

This will benefit the community as a whole because the emergency plan is a part of the community's total emergency plan. Emergency planning must be a part of overall business operations, just as security is.

Source: www.fema.gov/national-response-framework.

119. PLAN DEVELOPMENT AND PRIMARY CONSIDERATIONS

WHY EMERGENCY PLANNING?

Three primary goals:

1. Protection of lives
2. Protection or property
3. Restoration of operations

Risk assessment: consider probabilities and severity of each type of disaster occurring.

Government and industry must share burden of protecting the public.

Threat scenarios.

Most serious industrial hazards:

- Fire
- Explosion

Most common emergencies:

- Fire
- Bomb threat
- Labor dispute

Stages of emergency planning:

- Anticipate emergency
- Provide for responsive action
- Return to normal operations

Planning basics.

Emergency plans should be in writing.

Provide specific and precise actions.

No new organizations created at the time of disaster!

Identify who can declare emergency.

Identify the Emergency Coordinator.

Ensure continuity of leadership.

Basic plan has three essential elements:

- Authority
- Types of emergencies
- Execution

Outline plant shutdown procedures (to be carried out by Engineering).

Evacuation routes must remain consistent for all threats.
Test plan annually—brief every employee!
Table-top exercise with public safety involvement.
Create an ECC:
    Maps/procedure charts/call-up lists/MAAs.
    Backup power and communications gear.
Disaster response and medical gear.
Identify PR person to coordinate media.
Backup sites—hot, warm, cold.
Preserve vital records (2%)—bylaws, board minutes, stock transactions, financial data.
The most practical way to discover deficiencies is to test the plan annually.
Make the plan direct in nature.
Do not restrict the plan to senior management only.
Plan is typically activated by the Plant/Facility Manager or President/CEO.

TYPES OF EMERGENCIES: NATURAL AND MAN-MADE

Natural Disasters

Tornadoes (five classifications based on wind speeds (Fi–F5) of 200–400 mph—ground speeds of 30–70 mph)
    Width up to a mile—travel up to 30 miles
    "Tornado Watch"—tornado expected
    "Tornado Warning"—tornado sighted in area
Thunderstorms
    "Severe"—heavy rain, hail, and winds >50 mph
    "Severe watch" projected winds >75 mph
    Floods
Floods
    "Flash flood watch"—flooding is possible
    "Flash flood warning"—flooding is about to occur
Hurricanes (heavy rains—winds>74 mph) (five categories based on wind speeds)
    "Watch"—expected within 36 h
    "Warning"—expected within 24 h
Snowstorm
    "Heavy snow warning"—4"/12 h or 6"/24 h
    "Severe blizzard warning"—>45 mph
Earthquakes
    Unpredictable—can last as long as 5 min
    If inside, remain there; seek cover under heavy furniture in the center of the building
    "Tsunami" is a tidal wave caused by underwater earthquakes

Man-Made Disasters

- Plant fires
- Bomb threats
- Labor unrest
- Terrorism
- Sabotage
- Chemical/radiological accidents
- Transportation accidents
- Public demonstrations and civil disturbances
- Fire
  - Causes are preventable
  - Carelessness
  - Ignorance
  - Most are electrical in origin
  - Most fatalities are a result of toxic gas inhalation, followed by death from smoke inhalation and high temperatures.

CONCLUSION

Soft targets that are vulnerable or "at risk" need to be "hardened" to make them less attractive to criminals and/or terrorists. It is more difficult to protect targets and be prepared for an incident if the attack comes from within the organization, so ensure to have a plan if this does occur. An effective, comprehensive, Emergency Response Plan should be developed and training and drills should be conducted with staff and emergency responders to respond effectively to all emergency situations, whether they are natural or man-made or originate from the inside or the outside of the organization.

When determining vulnerability for man-made issues or natural phenomenon, we use foreseeability as one of the indicators that we need to take a proactive action. "Hoping for the best, being prepared for the worst and unsurprised by anything in between,"[15] is the best way to describe this process.

Source: Best Practices for Educational Environments: A 16 Point Master Plan, By Lawrence J. Fennelly, CPOI, CSSI, CHS-lll, CSSP-I & Marianna Perry, M.S., CPP, CSSP-I updated 2016.

120. EMERGENCY PLANNING BEST PRACTICES[16]

Develop an effective, comprehensive, Emergency Response Plan and provide training/education for the staff.

[15] www.goodreads.com/quotes.

[16] Fennelly LJ, Perry MA, Fagel MJ. Best Practices; copyrighted 2015.

Establish emergency procedures with standardized actions and directives for inclement weather (tornado, earthquake, hurricane, flooding, etc.), medical issues, fire, building evacuations, shelter-in-place, lockdown, workplace violence, and active shooter, as well as a business continuity plan for after the incident (OSHA, NFPA, FEMA, etc.).

Ensure your emergency procedures comply with ADA Standards [physically handicapped, vision and hearing impaired (special needs students, faculty, staff, if in a school setting), visitors, etc.]. Have designated individuals trained to assist.

Conduct regular training and joint exercises for emergency procedures with the local FD, PD, EMS and other local first responders. Provide floor plans for each building on the campus to each of these departments. Consider supplying building plans and layout of campus in a digital format for quicker access by more responders. Update the thumb drives on a quarterly basis that can be issued to teams. The main servers may be down, as well as cloud based, so a thumb drive for a laptop may be the only available tool (install in exterior locked Knox or Supra Boxes).

Establish a Crisis Management Team with documentation, training, and integration into the larger Incident Command Team. Determine who has the immediate authority to lockdown, issue a Clery alert for higher education and talk to the press. Establish a Joint Information Center with appropriately trained public information officer who can supply vetted information that comes from the command staff only.

The Crisis Management Team will integrate into the response and recovery operations and will work closely with the first responder community as the situation ebbs and flows.

Develop procedures for during and after a crisis situation.

Develop Mass Notification Procedures.

Provide two-way radios batteries, chargers, cases, and training (or another alternative method for communication) for staff, and establish a designated command center area or location.

The staff should follow the prescribed plan and report to the ECC or other predesignated area for response and recovery. This may not be at the same site due to safety reasons and may be at a remote location.

Administrators will need to be at different locations and not in the immediate area of the event for their own and response operations safety.

Ensure you are in compliance with all applicable OSHA regulations, Life Safety Codes, and local/state fire codes.

NFPA 1600 is a useful tool to help comply with for all risks and all hazards planning.

Provide FEMA training for administration and crisis team members.[17]

Conduct fire, evacuation, lockdown, shelter-in-place, etc., drills.

Consider using the standard response protocol, “I love u guys foundation.”

Develop crisis kits with all necessary supplies for an emergency situation.

Develop GO BAGS for action teams.

[17] www.training.fema.gov.

Establish markings, vests, hats, or other easy identification so that the school teams can be effectively identified to appropriate response officials.

Collaborate with local law enforcement and other emergency responders to determine if interior door windows are to be covered and/or if shades are to be left open or pulled down in a lockdown situation.

Develop an effective and practiced mutual aid agreement with other organizations and businesses.

Collaborate with local law enforcement and all emergency response officials to establish protocols for shades and green cards to determine if interior door windows are to be covered and/or if shades are to be left open or pulled down in a lockdown situation.

121. EMERGENCY RESPONSE AND LIFE SAFETY

THE PURPOSE OF EMERGENCY PLANNING AND WHAT GOES INTO THE PLAN

Protection of life
Protection of assets
Business continuity

122. INGRESS AND EGRESS CONTROLS CHECKLIST

PERSONAL GATE

1. Are the ingress and egress of employees and visitors adequately controlled?
2. Are employee identification (ID) badges properly checked?
3. Are visitors signing in, appointments of salesmen and other visitors verified, and visitor badges properly issued and returned when the visitors exit?
4. Are records being kept of employee's ID badges that have been reported lost or stolen?
5. Do employees sign in if their ID badges are lost or stolen, and is their arrival for scheduled work assignments verified with their immediate supervisors?
6. Are replacement ID badges being issued promptly for lost, stolen, or deteriorated ID badges?
7. When an employee changes his facial features by adding or deleting facial hair, glasses, or other characteristics that may alter his appearance, are new ID badges issued so that a current ID record is maintained?
8. Are package passes being checked to verify contents of packages?
9. Are briefcases, lunch boxes, insulated bottles, bags, etc., being checked by the Protection Officer?
10. Are all other requirements of the package-pass procedure being followed?

11. Are all other procedures prescribed in the personnel gate section of the Protection Officers' manual being complied with?
12. Controls:
    a. Facility planning/architectural layout and design
    b. Natural access control/designed access
    c. Electronic access control/access monitored and managed
    d. Security awareness/policy, procedures, best practices, and a master plan

123. MASS NOTIFICATION PROCEDURES

Develop a Mass Notification Program, which includes e-mails, text messages, social media, public address system announcements, as well as audible alarms. In the age of technology and digital communication, electronic message boards are becoming more common as a form of notification.

This must use prescripted messages, and messaging must be approved by the Incident Command Staff (not a committee) before being broadcast.

Ensure your Mass Notification Program complies with ADA Standards (physically handicapped, visually impaired, hearing impaired or special needs students, faculty, staff and visitors, etc.). Have designated individuals trained to assist. Provide language assistance and preestablished phone trees.

Ensure that your procedures meet NFPA Standards and Guidelines, which includes a communication program, an incident management system, and individuals who can effectively understand ICS and the procedures and protocols. There must be at least three people trained per position in the Emergency Management Organization.

Emergency notifications can be made via the public address system, or text to employees, but you may also want to consider a warning appearing on the screen of every computer that is on the company network. There should be redundant notification and communication systems and procedures. Keep in mind visually, hearing, or physically impaired individuals when considering emergency notification processes.

The following are recommendations that will strengthen mass notification practices at your complex:

1. Prerecorded messages: Prerecorded messages need to be developed to address the most likely and the most catastrophic emergency situations that will require utilization of mass notification systems. Furthermore, prerecorded messages will allow security officers to initiate mass notification, significantly reducing the time delay.
2. Protocol: Management must establish a clear protocol to address the following:
    a. Activation guidelines: Description of situations/criteria that require utilizing the CCC Alert system.
    b. Authority: Authority to activate CCC Alert must be given to security operators/dispatchers tasked with monitoring all of security systems. This will allow for quick and efficient mass notification in case of an emergency situation.

c. Practice: It is recommended that mass notification be included as part of any emergency drill conducted at your complex. This will prepare security operators to utilize mass notification in times of crisis. Furthermore, such ongoing practices will significantly reduce the amount of time it takes to send a message through the mass notification system.

124. REINVENTING SECURITY PERFORMANCE

Some time ago, we wrote that security assessments *should be conducted at times of crisis*. We have seen terrorist attacks in Paris, San Bernardo, and Brussels. We have also seen that the threat levels and security awareness increase in these areas.

Question: "What have you done recently to increase your level of security? An assessment? More training? Did you request that additional doors be secured? During these times of crisis, it is our recommendation that you also increase your level of protection. As national threat levels go up, so should your threat awareness.

It is during these times of crisis that security components get updated and additional security measures often get approved. Conducting annual or monthly security reviews and improving security at your site will fuel overall security performance. At times, security programs need a shot in the arm or a wake-up call. Increase the rounds made by your security officers within your complex to improve security coverage. Set up a schedule to check all alarm sensors and make sure they are working properly. Check also to ensure that all cameras are recording properly. All your security components must be operational and providing you with the best protection possible.

125. OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION[18]

"The Williams–Steiger Occupational Safety and Health Act of 1970 requires in part that every employer covered under the Act furnish his or her employees a place of employment which is free from recognized hazards that are causing or are likely to cause death or serious physical harm to his/her employees."

The enforcement of OSHA is the responsibility of either the Department of Labor (DOL) of the Secretary of Health and Human Services. The DOL is decentralized and operates out of regional, district, and maritime offices. OSHA encourages individual states to develop their own occupational health and safety plans as long as their program is as least as stringent as OSHA.

Prior to OSHA, there was no common national standard for safety. There is still no national standard for security, but ASIS International has standards, guidelines, and best practices for the security industry.

[18] www.osha.gov.

126. EMERGENCY PROCEDURES AND SECURITY OPERATIONS

The following 4 OSHA regulations may have a direct impact on security policies and procedures:

Means of Egress
29 CFR 1910.36
Medical Services and First Aid
29 CFR 1910.151
OSHA Publication - Best Practices Guide: Fundamentals of a Workplace First-Aid Program
Fire Protection
29 CFR 1910.151
Emergency Action Plans
29 CFR 1910.38

Some safety-related tasks are many times the responsibility of security/protection officers, for example, reporting blocked exits, administering cardiopulmonary resuscitation (CPR) and first aid, checking fire extinguishers monthly, and reporting slip/trip and fall hazards.

Security/protection officers and safety responsibilities:

Define the duties of personnel with an assigned role.
Establish procedures for each position.
Prepare checklists for all procedures.
Define procedures and responsibilities for firefighting, medical, and health.
Determine lines of succession to ensure continuous leadership, authority, and responsibility in key positions.
Determine equipment and supply needs for each response function.
Assign all personnel responsibility for:
- Recognizing and reporting an emergency
- Warning other employees in the area
- Taking security and safety measures
- Evacuating safely
- Providing training

127. OSHA FACT SHEET: EMERGENCY EXIT ROUTES

EMERGENCY EXIT ROUTES

How would you escape from your workplace in an emergency? Do you know where all the exits are in case your first choice is too crowded? Are you sure the doors will be unlocked and that the exit access behind them will not be blocked during a fire, explosion, or other crisis? Knowing the answers to these questions could keep you safe during an emergency.

WORKPLACE EXIT ROUTES

Usually, a workplace must have at least two exit routes for prompt evacuation. But more than two exits are required if the number of employees, size of the building, or arrangement of the workplace will not allow a safe evacuation. Exit routes must be located as far away as practical from each other in case one is blocked by fire or smoke.

REQUIREMENTS FOR EXITS

- Exits must be separated from the workplace by fire-resistant materials—that is, a 1-h fire-resistance rating if the exit connects three or fewer stories, and a 2-h fire-resistance rating if the exit connects more than three floors.
- Exits can have only those openings necessary to allow access to the exit from occupied areas of the workplace or to the exit discharge. Openings must be protected by a self-closing, approved fire door that remains closed or automatically closes in an emergency.
- Keep the line-of-sight to exit signs clearly visible always.
- Install "EXIT" signs using plainly legible letters.

SAFETY FEATURES FOR EXIT ROUTES

- Keep exit routes free of explosives or highly flammable furnishings and other decorations.
- Arrange exit routes so that employees will not have to travel toward a high-hazard area unless the path of travel is effectively shielded from the high-hazard area.
- Ensure that exit routes are free and unobstructed by materials, equipment, locked doors, or dead-end corridors.
- Provide lighting for exit routes adequate for employees with normal vision.
- Keep exit route doors free of decorations or signs that obscure their visibility of exit route doors.
- Post signs along the exit access indicating the direction of travel to the nearest exit and exit discharge if that direction is not immediately apparent.
- Mark doors or passages along an exit access that could be mistaken for an exit "Not an Exit" or with a sign identifying its use (such as "Closet").
- Renew fire-retardant paints or solutions when needed.
- Maintain exit routes during construction, repairs, or alterations.

DESIGN AND CONSTRUCTION REQUIREMENTS

- Exit routes must be permanent parts of the workplace.
- Exit discharges must lead directly outside or to a street, walkway, refuge area, public way, or open space with access to the outside.
- Exit discharge areas must be large enough to accommodate people likely to use the exit route.

- Exit route doors must unlock from the inside. They must be free of devices or alarms that could restrict use of the exit route if the device or alarm fails.
- Exit routes can be connected to rooms only by side hinged doors, which must swing out in the direction of travel if the room may be occupied by more than 50 people.
- Exit routes must support the maximum permitted occupant load for each floor served, and the capacity of an exit route may not decrease in the direction of exit route travel to the exit discharge.
- Exit routes must have ceilings at least 7 ft, 6 in. high.
- An exit access must be at least 28 inches wide at all points. Objects that project into the exit must not reduce its width.

Source: www.osha.gov.

128. OSHA FACT SHEET: FIRE SAFETY IN THE WORKPLACE

FIRE SAFETY IN THE WORKPLACE

What should employers do to protect workers from fire hazards? Employers should train workers about fire hazards in the workplace and about what to do in a fire emergency. If you want your workers to evacuate, you should train them on how to escape. If you expect your workers to use firefighting equipment, you should give them appropriate equipment and train them to use the equipment safely (see Title 29 of the Code of Federal Regulations Part 1910 Subparts E and L; and Part 1926 Subparts C and F). What does OSHA require for emergency fire exits? Every workplace must have enough exits suitably located to enable everyone to get out of the facility quickly. Considerations include the type of structure, the number of persons exposed, the fire protection available, the type of industry involved, and the height and type of construction of the building or structure. In addition, fire doors must not be blocked or locked when employees are inside. Delayed opening of fire doors, however, is permitted when an approved alarm system is integrated into the fire door design. Exit routes from buildings must be free of obstructions and properly marked with exit signs. See 29 CFR Part 1910.36 for details about all requirements. Do employers have to provide portable fire extinguishers? No. But if you do, you must establish an educational program to familiarize your workers with the general principles of fire extinguisher use. If you expect your workers to use portable fire extinguishers, you must provide hands-on training in using this equipment. For details, see 29 CFR Part 1910 Subpart L. Must employers develop emergency action plans? Not every employer is required to have an emergency action plan. OSHA standards that require such plans include the following:

- Process Safety Management of Highly Hazardous Chemicals, 1910.119,
- Fixed Extinguishing Systems, General, 1910.160
- Fire Detection Systems, 1910.164
- Grain Handling, 1910.272

- Ethylene Oxide, 1910.1047
- Methylenedianiline, 1910.1050
- 1,3 Butadiene, 1910.1051

When required, employers must develop emergency action plans that:

- Describe the routes for workers to use and procedures to follow.
- Account for all evacuated employees.
- Remain available for employee review.
- Include procedures for evacuating disabled employees.
- Address evacuation of employees who stay behind to shut down critical plant equipment.
- Include preferred means of alerting employees to a fire emergency.
- Provide for an employee alarm system throughout the workplace.
- Require an alarm system that includes voice communication or sound signals such as bells, whistles, or horns.
- Make the evacuation signal known to employees.
- Ensure emergency training.
- Require employer review of the plan with new employees and with all employees whenever the plan is changed.

Must employers have a fire prevention plan? OSHA standards that require fire prevention plans include the following:

- Ethylene Oxide, 1910.1047
- Methylenedianiline, 1910.1050
- 1,3 Butadiene, 1910.1051

Employers covered by these standards must implement plans to minimize the frequency of evacuations. All fire prevention plans must:

- Be available for employee review.
- Include housekeeping procedures for storage and cleanup of flammable materials and flammable waste.
- Address handling and packaging of flammable waste (recycling of flammable waste such as paper is encouraged).
- Cover procedures for controlling workplace ignition sources such as smoking, welding, and burning.
- Provide for proper cleaning and maintenance of heat-producing equipment such as burners, heat exchangers, boilers, ovens, stoves, and fryers, and storage of flammables away from this equipment.
- Inform workers of the potential fire hazards of their jobs and plan procedures.
- Review plan with all new employees and with all employees whenever the plan is changed. What are the rules for fixed extinguishing systems? Fixed extinguishing systems throughout the workplace are among the most reliable fire fighting tools. These systems detect fires, sound an alarm, and send water to the fire and heat. To meet OSHA standards, employers who have these systems must:

- Substitute (temporarily) a fire watch of trained employees to respond to fire emergencies when a fire suppression system is out of service.
- Ensure that the watch is included in the fire prevention plan and the emergency action plan.
- Post signs for systems that use agents (e.g., carbon dioxide, Halon 1211) posing a serious health hazard.

Source: www.osha.gov.

129. OSHA EMERGENCY PROCEDURES AND SECURITY OPERATIONS

PLANNING AND RESPONDING TO WORKPLACE EMERGENCIES

Nobody expects an emergency or disaster. Yet emergencies and disasters can strike anyone, anytime, anywhere. Employers should establish effective safety and health management systems and prepare their workers to handle emergencies before they arise.

Planning is required by some OSHA standards; firms with more than 10 employees must have a written emergency action plan, whereas smaller companies may communicate their plans orally. Top management support and the commitment and involvement of all employees are essential to an effective emergency action plan. Employers should review plans with employees when initially put in place and reevaluate and amend the plan periodically whenever the plan itself, or employee responsibilities, change. Emergency procedures, including the handling of any toxic chemicals, should include:

- Escape procedures and escape route assignments.
- Special procedures for employees who perform or shut down critical plant operations.
- Systems to account for all employees after evacuation and for information about the plan.
- Rescue and medical duties for employees who perform them.
- Means for reporting fires and other emergencies.

Chain of command: The employer should designate an emergency response coordinator and a backup coordinator. The coordinator may be responsible for plant-wide operations and public information and ensuring that outside aid is called. Having a backup coordinator ensures that a trained person is always available. Employees should know who the designated coordinator is. Duties of the coordinator and employer include:

- Determining what emergencies may occur and seeing that emergency procedures are developed to address each situation.
- Directing all emergency activities including evacuation of personnel.

- Ensuring that outside emergency services are notified when necessary.
- Directing the shutdown of plant operations when necessary.

Emergency Response Teams: Emergency response team members should be thoroughly trained for potential crises and physically capable of carrying out their duties. Team members need to know about toxic hazards in the workplace and be able to judge when to evacuate personnel or when to rely on outside help (e.g., when a fire is too large to handle). One or more teams must be trained in:

- Use of various types of fire extinguishers.
- First aid, including CPR and self-contained breathing apparatus.
- Requirements of the OSHA blood-borne pathogens standard.
- Shutdown procedures.
- Chemical spill control procedures.
- Search and emergency rescue procedures.
- Hazardous materials, emergency response its vital to have Effective emergency communication. An alternate area for a communications center other than management offices should be established in the plans, and the emergency response coordinator should operate from this center. Management should provide emergency alarms and ensure that employees know how to report emergencies. An updated list of key personnel and off-duty telephone numbers should be maintained.

Accounting for personnel following evacuation is critical. A person in the control center should notify police or emergency response team members of persons believed missing. Effective security procedures can prevent unauthorized access and protect vital records and equipment. Duplicate records of essential accounting files, legal documents, and lists of employee relatives—to be notified in case of emergency—can be kept at off-site locations.

Training: Every employee needs to know details of the emergency action plan, including evacuation plans, alarm systems, reporting procedures for personnel, shutdown procedures, and types of potential emergencies. Any special hazards, such as flammable materials, toxic chemicals, radioactive sources, or water-reactive substances, should be discussed with employees. Drills should be held at random intervals, at least annually, and should include outside police and fire authorities. Training must be conducted at least annually and when employees are hired or when their job changes. Additional training is needed when new equipment, materials, or processes are introduced; when the layout or design of the facility changes; when procedures have been updated or revised; or when exercises show that employee performance is inadequate.

Personal Protection: Employees exposed to or near accidental chemical splashes, falling objects, flying particles, unknown atmospheres with inadequate oxygen or toxic gases, fires, live electrical wiring, or similar emergencies need appropriate personal protective equipment (PPE).

Medical Assistance: First aid must be available within 3–4 min of an emergency. Work sites more than 3–4 min from an infirmary, clinic, or hospital should have at least one person on-site trained in first aid (available all shifts), have medical personnel readily

available for advice and consultation, and develop written emergency medical procedures. It is essential that first aid supplies are available to the trained first aid providers, that emergency phone numbers are placed in conspicuous places near or on telephones, and that prearranged ambulance services for any emergency are available. It may help to coordinate an emergency action plan with the outsider responders such as the fire department, hospital emergency room, EMS providers, and local HAZMAT teams.

Source: www.osha.gov.

130. AMERICANS WITH DISABILITIES ACT[19] COMPLIANCE AND SECURITY OPERATIONS

- Hallways and doorways that are used for egress as part of an accessible route shall be 36" wide.
- Accessible stairwells shall be 48" wide.
- Changes in levels greater than ½" shall have a ramp.
- Changes in levels between ¼" and ½" shall have a beveled edge.
- Fifty percent of all public entrances to a building shall be handicapped accessible.
- If emergency warning systems are provided, they shall have both audible and visual alarms.
- A round doorknob can be replaced with a lever handle or modified by adding a clamp-on lever.
- Locate accessible parking spaces as close as possible to the accessible entrances and on an accessible route to the building.
- Install a sign with the international symbol of accessibility and mount high enough so that the sign is not hidden by a vehicle parked in the space.
- ADA compliance provides for:
  - Clear explanations of the definitions of disability, reasonable accommodation, substantially limited, major life activities, undue hardship, readily achievable barrier removal, program accessibility, and all the other key terms in the law.
    - Steps to take to ensure ongoing compliance, specifically for state and local governments, businesses that are open to the public, and transportation authorities.

131. EMERGENCY POLICIES AND PROCEDURES TRAINING[20]

When hired, conduct classroom training on the policies and procedures of the organization. Repeat annually at in-service training or as necessary.

[19] http://www.ada.gov.

[20] Fennelly LJ, Perry MA, Fagel MJ. Best Practices for Schools; 2016.

Schedule annual miniexercises (not for failure but for reinforcement).
Schedule regular active shooter reaction training.
Develop a policy for faculty and staff about when to use a fire extinguisher. OSHA Regulations state that if a person is *required* to use an extinguisher as part of his or her duties, the person must be adequately trained in fire extinguisher operation and selection. If fire extinguisher use is voluntary and not required, then the training obligation is diminished.
Always insist that upon discovery of any fire, regardless of the size, to notify the Fire Department and sound the appropriate alarm.
Discuss when to fight a fire or when to flee a fire.
Train staff on how to use a fire extinguisher. Adequately train per OSHA and state regulations.
Conduct First Aid, CPR/AED and Bloodborne Pathogens Training (29 CFR 1910. 151) and repeat recertification as required. Understand whether or not giving first aid is a requirement vs. voluntary, as this involves Heptavac vaccine, training, PPE, and appropriate universal precautions.
Conduct training on how to respond to medical issues, fire, inclement weather, building evacuations, shelter-in-place, lockdown, workplace violence, active shooter, etc. Appropriately trained staff will educate students as to the appropriate policies.
Ask local, state, and federal agencies to participate in your tabletop or incident training.

132. ELEVATOR AND ESCALATOR SAFETY ISSUES[21]

ELEVATORS

There are safety precautions to remember regarding elevators. When passengers approach a closing elevator door, they should never extend a hand or any other object to stop it. Not all elevator doors will reopen, and an arm could get caught between the moving doors. To avoid tripping, passengers should check the entrance floor to make sure the elevator car is level with the floor.

Occasionally, elevators do get stuck between floors. However, the odds of getting stuck in an elevator are about once in a lifetime for the average person using an elevator daily. lf passengers find themselves trapped in an elevator, they must be patient, use the emergency phone to call for help, and follow the instructions of responding trained professionals. Passengers need to know there is plenty of air in the elevator, so they should stay calm. Caution them never to climb out of an elevator. There is always the danger of falling down the elevator shaft. Post appropriate instructions and advise building tenants of proper procedures.

[21] www.eesf.org.

Proper installation and ongoing maintenance and inspection are imperative when ensuring elevator safety. However, facilities professionals should also make sure employees know the proper riding procedures and how to recognize improper behavior. In addition, tenants and visitors need to be periodically reminded of safe riding procedures. A proactive approach to safety education for employees, tenants, and visitors can reduce potential accidents.

ESCALATORS

As a rule, small children should never ride alone, and parents or guardians should ensure that a child's feet are in the center of the step. Children should also not sit down on an escalator, because loose clothing can get pulled into the moving steps. Machinery will continue to pull and tug, unless the child is freed from the clothing or the escalator is turned off. Young riders who can comfortably reach the handrail should do so to maintain balance. However, if they are too small to hold the handrail without being pulled against the side of the escalator, they should only ride holding someone's hand.

Dangerous mishaps also happen when passengers push baby strollers on escalators. This activity potentially allows for the stroller and/or the child to fall causing serious injury, especially on the "down" escalator. It is much safer to take an elevator when arms are overloaded.

Senior citizens are another group of escalator riders needing special attention. Individuals who use walkers, are unsteady on their feet, take medication, or have an illness that affects eyesight, mobility, or balance should ride the elevator instead of the escalator.

ELEVATOR SAFETY

Watch your step
Leave closing doors alone
If doors do not open when you are on an elevator, put the alarm button and wait for assistance
If there is a fire in the building, use the stairs

ESCALATOR (AND MOVING WALKWAY) SAFETY

Step on and off carefully; people only—no canes, walkers, or wheeled vehicles
Hold the handrail
Hold children or small packages firmly with one hand
Do not touch the sides below the handrail
Stand facing forward

For more information on safety education programs contact: The Elevator Escalator Safety Foundation, 356 Morgan Ave., Mobile, AL 36606.

133. UNSAFE ACTS AND UNSAFE CONDITIONS[22]

Accidents are caused either by unsafe acts or unsafe conditions:

People not thinking, not following instructions, or not putting their training into practice.
Unsafe manual handling, loading, stacking, and storing of materials.
Overloading of platforms, scaffolds, hoists, plant, etc.
Use of faulty equipment and "homemade" repairs.
Illegal adaptions and illegal removal of guards/barriers.
Failure to use PPE and ignoring safety signs/warning devices.

The costs of accidents include pain, suffering, ongoing disability, and potential fatalities.

Accidents are grouped into two categories:
Accidents that happened due to "unsafe conditions"
Accidents that happened due to "unsafe acts"
Unsafe conditions:
- Every activity has certain inherent potential for accidents.
- Unless care is taken, accidents are bound to happen
- To avoid accidents steps must be taken, such as
  - Follow the defined procedures,
  - Use the recommended safety gadgets
  - Adhere to the safety instructions.

In spite of adhering to the aforementioned rules, accidents may occur due to uncontrollable reasons and are beyond the controls of the operator.

Unsafe acts:
- These are due to the fault of the persons engaged in the work.
- They occur due to:
  - Not following safety rules
  - Not using proper safety gadgets.

During a job interview, the security supervisor applicant asked the facilities manager if they were having any problems with crime. He was told that crime was not a problem, but that they did have quite a few slip-and-fall accidents, especially during the winter on the ice. After the security supervisor was hired, he instructed the security officers on patrol to continuously inspect for icy areas and to distribute ice melt granules if ice was discovered. You may call this job safety, but the idea is to be proactive—identify unsafe conditions and to then control the hazards. Less slip-and-fall accidents meant fewer employee injuries, and also less report writing for the security officers. Many times it is the responsibility of security/protection officers to be vigilant and constantly inspect the area for unsafe conditions or areas in need of attention. Security/protection officers

[22] https://www.linkedin.com/pulse/20141012213715-52718218-unsafe-act-and-unsafe-condition.

can either control or eliminate hazards by reporting it to the proper department or by being proactive and taking care of minor issues, such as applying ice melt, as in the aforementioned example.

134. FIFTY THINGS YOU SHOULD KNOW: A CHECKLIST

Ensure that exterior doors into inhabited areas open outward. Ensure emergency exit doors only facilitate exiting.

1. Secure room access hatches from the interior. Prevent public access to building roofs.
2. Restrict access to building operation systems.
3. Conduct periodic training of HVAC operations and maintenance staff.
4. Evaluate HVAC control options.
5. Install empty conduits for future security control equipment during initial construction or major renovation.
6. Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls.
7. Minimize interior glazing near high-risk areas.
8. Establish written plans for evacuation and sheltering in place.
9. Integrating multiple security systems in a layered effect, including CPTED.
10. Illuminate building access points.
11. Restrict access to building information.
12. Secure HVAC intakes and mechanical rooms.
13. Limit the number of doors used for normal entry/egress.
14. Lock all utility access openings.
15. Provide emergency power for emergency lighting in restrooms, egress routes, and any meeting room without windows.
16. Install a modern public address system that will direct individuals where to go in case of an emergency. Have several modes of emergency notification.
17. Stagger interior doors and offset interior and exterior doors.
18. Eliminate hiding places.
19. Install a second and separate telephone service.
20. Install radio telemetry distributed antennas throughout the facility.
21. Use a badge identification system for building access.
22. Install a CCTV security surveillance system.
23. Install an electronic security alarm system.
24. Install rapid response and isolation features into HVAC systems.
25. Use interior barriers to differentiate levels of security.
26. Locate utility systems away from likely areas of potential attack.
27. Install duress alarms at key public contact areas.
28. Install emergency and normal electric equipment at different locations.
29. Avoid exposed structural elements.

30. Reinforce foyer walls.
31. Use architectural features to deny contact with exposed primary vertical load members.
32. Isolate lobby areas, mailrooms, loading docks, and storage areas.
33. Elevate HVAC fresh-air intakes.
34. Ensure that emergency generator exhaust pipes are not located in close proximity to HVAC air intakes.
35. Create "shelter-in-place" rooms or areas.
36. Define HVAC zones. Eliminate leaks and increase building air tightness.
37. Install blast-resistant doors or steel doors with steel frames.
38. Physically separate unsecured areas from the main building.
39. Install HVAC exhausting and purging systems.
40. Connect interior non–load-bearing walls to structure with nonrigid connections.
41. Use structural design techniques to resist progressive collapse.
42. Treat exterior shear walls as primary structures.
43. Orient glazing perpendicular to the primary facade facing uncontrolled vehicle approaches.
44. Effectively place bollards to prevent vehicle access into buildings.
45. Use reinforced concrete wall systems in lieu of masonry or curtain walls.
46. Ensure that an active fire detection and suppression system is protected from single-point failure in case of a blast event.
47. Designate a backup control center.
48. Harden eaves and overhangs to withstand blast effects.
49. Establish designated group floor elevation 4 feet above grade.
50. Secure all openings to building within 14 feet of ground level or within 14 feet of access to roof.

Integrating multiple security systems in a layered effect—including CPTED and environmental security, critical infrastructure protection, building designs, interior/exterior layout, detection systems, structural barriers, access controls, communications, and video surveillance—contributes to the protection of assets as well as the control and reduction of losses.

PART

Emerging Trends 5

135. SOCIAL MEDIA: TRANSFORMING OUR CULTURE

We are not only in the digital technology age, but also in the age of social media. Our culture has been affected by this phenomenon. Many managers jump online before they even brush their teeth!

Social media has helped to bind groups and communities together. We have more linked-in security groups online than we ever knew existed, and this group culture has expanded with active participants.

For the Security Cultural Community, the groups discuss issues, books, events, and knowledge. They ask questions and seek answers and certifications. Leaders and leadership strategies are developed. Consultants get a boost and audiences are formed. Some may call this crowd culture. Webinars and conferences are promoted online as well as by presenters.

Security companies offer a wide variety of online white papers touting their latest technology and use this as a means of promoting their brand of products. Professional public relations firms are busier than ever because a new media outlet is now available to them.

We are seeing this person and that person with five million followers! Our American Society for Industrial Security (ASIS) School Safety and Security Council in less than a year old and has 4000 followers, and the group is becoming larger each month! But what is the ultimate goal? What are the long-term objectives? Where will all of the growth come from? Moving ahead strategies will be developed taking the social media culture to the next level.

Since we are talking about social media, we would be remiss to not mention some things about online safety. We all can use a few reminders on Internet safety. The following information is taken from www.fbi.gov. Internet-based social networking sites have created a revolution in social connectivity. However, con artists, criminals, and other dishonest actors are exploiting this capability for nefarious purposes. There are primarily two tactics used to exploit online social networks. In practice, they are often combined:

1. Computer-savvy hackers who specialize in writing and manipulating computer code to gain access or install unwanted software on your computer or phone.
2. Social or human hackers who specialize in exploiting personal connections through social networks. Social hackers, sometimes referred to as "social engineers," manipulate people through social interactions (in person, over the phone, or in writing). Humans are a weak link in cyber security, and hackers and

Physical Security: 150 Things You Should Know. http://dx.doi.org/10.1016/B978-0-12-809487-7.00005-X

social manipulators know this. They try to trick people into getting past security walls. They design their actions to appear harmless and legitimate. Falling for an online scam or computer hack could be damaging for an individual victim as well as the organization the victim works for.

VULNERABILITY OF SOCIAL NETWORKING SITES

Social networking sites are Internet-based services that allow people to communicate and share information with a group.

Risks

Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high-security settings, friends or websites may inadvertently leak your information. Personal information you share could be used to conduct attacks against you or your associates. The more information shared, the more likely someone could impersonate you and trick one of your friends into sharing personal information, downloading malware, or providing access to restricted sites. Predators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation.

Information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site.

136. ENCRYPTION

ENCRYPTION DEFINED

In his book, Integrated Security Systems Design, on page 137, Thomas Norman, CPP, PSP, CSC defined encryption as a process of replacing clearly written text language (clear text) with a substitute of mixed up characters (or even a pixelated image) so that the meaning of the text is obscured. The intended recipient of the text is restricted from reading the text. The intended recipient will have been provided a key to unlock the readable text from the garbled letters numbers or pixelated text so the message can be read.

Source: Norman, T, CPP, PSP, CSC, B-H. Integrated Security Systems Design. 1st ed.; 2007. p. 137.

137. CYBER THREATS

Inge Sebyan Black, CPP, CFE, CCIE, CPOI, CEM

Technology has become a target, a vulnerability, and a tool used by criminals and terrorists, and cyber threats continue to be significant areas of concern. In 2012, the US Intelligence Community expressed increasing concern about cyber threats,

indicating that such threats are likely to increase in coming years and eventually constitute the number one threat to the United States.

Terrorists are increasingly cyber savvy, using the Internet to recruit members and supporters, disseminate information, plan operations, and communicate with each other. Hostile foreign nations use cyber tools as a means of espionage as they target sensitive information from governments and businesses. Some cyber criminals target individuals and companies for financial gain, whereas others steal information and cause damage with ideological motivations.

Cyber threats, to include cyber terrorism, cyber warfare, and cyber crime, are increasingly becoming a major threat to the nation's security and show no signs of slowing down. Emerging technologies and the move toward cloud computing, although presenting new opportunities and ease of use, are providing new avenues of exploitation and vulnerability. Cyber threats range from benign low-risk threats that are easily mitigated by current technology to high-risk threats requiring sophisticated countermeasures. Cyber threats can cause massive financial losses, degrade or disrupt services, facilitate extortion, facilitate intellectual property theft, and facilitate identity theft.

We are particularly concerned about the potentially severe consequence of an effective cyber attack against a state agency that could result in denial or disruption of essential services, including utilities, public health, firefighting, and law enforcement. For example, the Texas Department of Public Safety was targeted in thousands of cyber attacks during 2012. This threat underscores the importance of system redundancies and backup capabilities, given the importance of DPS (Department of Police Services) information technology systems for the law enforcement and criminal justice system across the state, although any network disruption would also compromise the issuance of driver licenses, concealed handgun licenses, and other essential state services. Other state agencies also provide essential services and likely face comparable threats and consequences from cyber attacks.

Some common types of cyber activity include the use of botnets, denial of service, hacking, key stroke logging, malware, phishing, and other activities.

138. CYBER THREAT ACTORS

Inge Sebyan Black, CPP, CFE, CCIE, CPOI, CEM

The cyber threat encompasses actors on many different levels.

Nation-states: Many nations have some form of information operations capability and are developing greater capability and operational reach every day.

Terrorists: Terrorists use cyber technology for communications, financing, intelligence gathering, planning, propaganda, radicalization, recruitment, and training.

Insiders: Insiders have the potential to cause grave damage due to their access and knowledge of the systems.

Hacktivists: Hacktivists are politically or ideologically motivated cyber actors who conduct website defacements, redirects, denial-of-service attacks, information theft, virtual sabotage, website parodies, and software development.

Cyber criminals: Cyber criminals are financially motivated, and will work for whoever will pay.

Although the cyber threat from hostile foreign nations is a high-profile, persistent issue to our national security, sophisticated cyber crime continues to be a ubiquitous threat that is adversely affecting our financial health and potentially endangers public safety.

Critical infrastructure networks are potential cyber targets. The industrial control systems of critical infrastructure may be vulnerable to attack due to growing interconnectedness.

139. CYBER CRIME: WHAT SECURITY DIRECTORS NEED TO KNOW ABOUT CYBER SECURITY

Inge Sebyan Black, CPP, CFE, CCIE, CPOI, CEM

Security directors today must know, first and foremost, that their company will be a victim of a cyber attack. These attacks will be both complicated and costly. The company should be prepared to preserve digital forensics, conduct investigations, provide notification to a broad range of parties, comply with state and federal compliance obligations, and prepare for what could be potential litigation. Did I mention that there may be a need to plan for possible credit monitoring, crisis management, and of course, defending all actions to the Board of Directors? The security director's most important job is to communicate, to the Board of Directors or CEO, that information security should be established and maintain a high profile. Be prepared to ensure that auditing and regulatory compliance is not only visible but also the highest priority.

Security directors are obligated to understand cyber security and to keep it as a priority. It is crucial to gain allies in various departments such as audit, business continuity, infrastructure, compliance, and finance, because they will help make the case that a cyber attack is an enterprise-wide issue.

Security directors, who are educated in information security and understand the threats, are better able to plan for IT security budgeting and training programs and appropriately design physical and IT security. It will be critical for them to know how they should react to a cyber attack and the steps they need to take.

The security director must understand the new reality facing boards of directors across the country—the emerging cyber security threats, the potential liability, and the probability of government enforcement actions.

140. BODY CAMERAS FOR LAW ENFORCEMENT AND THE PRIVATE SECTOR

Body cameras have quickly become a hot-button issue for law enforcement and policymakers, and now they are poised to become a private security and insurance issue

too. There is certainly a chance for increased liability with the use of body cameras among private security officers, but in the long run, it may be a boon to insurers, security guard companies, and the people they protect.[1]

LEGAL ISSUES WITH AUDIO RECORDING

Some states require only one person (i.e., person wearing the recording device), whereas others require two people to know that a conversation is being recorded. Visual recording and audio recording legal requirements do not always align.

TRAINING

Training is required so that officers and security will know where and when they can legally record a person. Privacy and the "expectation of privacy" must be understood by those wearing body video technologies.

DEPARTMENT

Officers and security guards who wear video technology are more likely to act appropriately and maintain their composure.

141. MARIJUANA: THE PROS AND THE CONS

Marijuana is obtained from the dried leaves, flowers, stems, and seeds of the hemp plant, *Cannabis sativa*. The plant contains the mind-altering chemical, delta-9-tetrahydrocannabinol (THC). Extracts with high amounts of THC can also be made from the cannabis plant.[2] The THC in marijuana is the chemical responsible for most of marijuana's psychological effects because it acts much like the cannabinoid chemicals made naturally by the human body. The cannabinoid receptors are concentrated in the areas of the brain associated with thinking, pleasure, coordination, and time perception. The THC in marijuana attaches to these receptors and activates them and affects a person's memory, pleasure, movements, thinking, concentration, coordination, and sensory and time perception.[3]

Marijuana is the third most popular recreational drug in the United States, behind alcohol and tobacco, according to the marijuana reform group NORML, and they state that marijuana is less dangerous than alcohol or tobacco because approximately 50,000 people die each year from alcohol poisoning and more than 400,000 deaths each year are attributed to tobacco use. By comparison, marijuana is nontoxic and cannot cause death by overdose.[4] NORML supports a legally

[1] Tory Brownyard, 2015. http://www.securitymagazine.com/authors/1806-tory-brownyard.
[2] https://www.drugabuse.gov/publications/drugfacts/marijuana.
[3] http://www.livescience.com/24553-what-is-thc.html.
[4] http://norml.org.

controlled market for marijuana where consumers can buy marijuana for recreational use from a safe legal source.

The legalization of marijuana, whether it is for medical or recreational use, is a controversial subject. There are pros and cons of the argument, and each side cites research data supporting their stance on the subject that the other calls "low quality." Proponents say that marijuana helps and economy and the job market, and others say that it causes more crime and puts people at risk. The bottom line is that marijuana use can be good or bad, depending upon who you ask. For these reasons, the debate over marijuana continues.

142. SHOULD MARIJUANA BE LEGAL FOR MEDICINAL AND/OR RECREATION PURPOSES?

Voters in several states across the nation have been asked to decide whether marijuana should be legalized to be used as a medicine, but the National Cancer Institute states that marijuana has been used for medicinal purposes for over 3000 years.[5] Voters made their decisions about the legalization of marijuana for medicinal purposes on the basis of medical anecdotes, beliefs about the dangers of illicit drugs, and a smattering of inconclusive science. To help policymakers and the public make better-informed decisions, the White House Office of National Drug Control Policy asked the Institute of Medicine (IOM) to review the scientific evidence and assess the potential health benefits and risks of marijuana.

The IOM report, *Marijuana and Medicine: Assessing the Science Base*, released in March 1999, found that the THC in marijuana is potentially effective in treating pain, nausea, and vomiting and AIDS-related loss of appetite. They add that additional research involving clinical trials need to be conducted. The report also states that the therapeutic effects of smoked marijuana are modest and there may be medicines that are more effective. The report acknowledges that there are some patients who do not respond well to other medications they may "have no effective alternative to smoking marijuana."[6]

The IOM report stated the following findings:

> *The profile of cannabinoid drug effects suggests that they are promising for treating wasting syndrome in AIDS patients. Nausea, appetite loss, pain, and anxiety are all afflictions of wasting, and all can be mitigated by marijuana. Although some medications are more effective than marijuana for these problems, they are not equally effective in all patients.*
>
> *A rapid-onset (that is, acting within minutes) delivery system should be developed and tested in such patients. Smoking marijuana is not recommended. The long-term harm caused by smoking marijuana makes it a poor drug delivery system, particularly for patients with chronic illnesses.*

[5] http://www.livescience.com/24553-what-is-thc.html.
[6] http://medicalmarijuana.procon.org/view.answers.php?questionID=255.

Terminal cancer patients pose different issues. For those patients the medical harm associated with smoking is of little consequence. For terminal patients suffering debilitating pain or nausea and for whom all indicated medications have failed to provide relief, the medical benefits of smoked marijuana might outweigh the harm.[7]

Most research studies on both sides of the issue do agree that smoked marijuana is not a completely safe substance. It is a drug that when used, can produce a variety of effects. However, except for the harm associated with smoking, the adverse effects of marijuana use are within the range tolerated for other medications. The OEM (Office of Emergency Management) has cautiously endorsed the medical use of marijuana, but smoked marijuana is a crude way to deliver THC because it also delivers harmful substances. Based on this information it appears as though marijuana does have medical value, but its therapeutic components must be used in conjunction with conventional therapy to be safe and useful.

The Food and Drug Administration (FDA) has not approved smoked marijuana as a safe and effective drug, but recognizes that patients are looking for treatment options for some conditions such as nausea and vomiting caused by chemotherapy. Even though the FDA has not approved botanical marijuana because they have not found it safe and effective, they do, however; recognize the interest in using marijuana for medicinal purposes.[8] The FDA has approved the drug, Dronabinol, which is a medicine made from THC, is a light yellow resinous oil that is extracted from the marijuana plant.[9] It is used to treat or prevent the nausea and vomiting associated with chemotherapy to increase the appetites of patients with AIDS.

The American Lung Association does encourage continued research into the benefits, risks, and safety of marijuana use for medicinal purposes. They recommend that patients who are considering marijuana for medicinal purposes should make an informed decision by consulting with their doctors and also consider other methods of administration other than smoking.[10]

In 2014, Colorado was the first state to allow the sale of marijuana for recreational use to anyone aged 21 years or older. Marijuana sold at retail stores carries a 25% state tax, plus the Colorado state sales tax of 2.9%, which makes recreational marijuana one of the most heavily taxed consumer products in Colorado.[11]

As of June 19, 2015, 23 states and the District of Columbia had laws legalizing marijuana use in some form. Four states and the District of Columbia have legalized marijuana for recreational use. Many states have decriminalized the possession of small amounts of marijuana for recreational use, whereas others have passed medical marijuana laws allowing for limited use. Some medical marijuana laws are broader than others and list specific medical conditions that allow for treatment, but this varies from state to state. There are some states that have passed laws allowing residents

[7] http://medicalmarijuana.procon.org/view.answers.php?questionID=255.
[8] http://www.fda.gov/NewsEvents/PublicHealthFocus/ucm421163.htm.
[9] http://www.livescience.com/24553-what-is-thc.html.
[10] http://www.lung.org/stop-smoking/smoking-facts/marijuana-and-lung-health.html.
[11] http://www.cnn.com/2013/12/28/us/10-things-colorado-recreational-marijuana/.

to possess cannabis oil if they have certain medical illnesses. For example, Virginia has laws that allow the possession of marijuana as long as the individual has a prescription from a doctor. Federal law prohibits doctors from prescribing marijuana, so basically the state laws are not valid. This means that doctors can write a recommendation for medical marijuana, but not a prescription.[12] Although possession, sale, and consumption of marijuana remain illegal at the federal level, it is permitted for recreational use in four US states: Alaska, Colorado, Oregon, and Washington, plus the US capital, Washington DC.[13]

It is common knowledge that smoke is harmful to lung health. It does not matter whether the smoke is from burning wood, tobacco, or marijuana because toxins and carcinogens are released from combustion. Smoke from marijuana combustion has been shown to contain many of the same toxins, irritants, and carcinogens as tobacco smoke. Because marijuana smokers tend to inhale more deeply and hold their breath longer than cigarette smokers, there is greater exposure. Marijuana smoke injures the cell lining of the large airways, and many marijuana smokers have symptoms such as a chronic cough, phlegm production, wheezing, and acute bronchitis.[14]

Smoking marijuana affects the immune system and the body's ability to fight disease, especially for individuals with weakened immune systems or those taking immunosuppressive drugs. Smoking marijuana also kills the cells in the lungs that help remove dust and germs, which may lead to an increased risk of lower respiratory tract infections.[15]

THE SHORT-TERM EFFECTS OF MARIJUANA

The THC in marijuana passes from the lungs into the bloodstream and stimulates the receptors in the parts of the brain. This causes the "high" that users feel. Other effects include:

Altered senses (for example, seeing brighter colors)
Altered sense of time
Changes in mood
Impaired body movement
Difficulty with thinking and problem solving
Impaired memory

THE LONG-TERM EFFECTS OF MARIJUANA

Marijuana also affects brain development. When teenagers use marijuana, it may permanently affect their thinking, memory, and learning functions.[16]

[12] http://www.governing.com/gov-data/state-marijuana-laws-map-medical-recreational.html.
[13] http://www.taipeitimes.com/News/biz/archives/2016/03/06/2003640899.
[14] http://www.taipeitimes.com/News/biz/archives/2016/03/06/2003640899.
[15] http://www.lung.org.
[16] https://www.drugabuse.gov/publications/drugfacts/marijuana.

Long-term marijuana use has also been linked to mental illnesses and mental health problems, such as:

Temporary *hallucinations*—sensations and images that seem real, although they are not
Temporary *paranoia*—extreme and unreasonable distrust of others
Worsening symptoms in patients with *schizophrenia* (a severe mental disorder with symptoms such as hallucinations, paranoia, and disorganized thinking)
Depression
Anxiety
Suicidal thoughts among teens[17]

IS MARIJUANA ADDICTIVE?

Marijuana can be addictive. Research suggests that about 1 in 11 users becomes addicted to marijuana.[18,19] This number increases among those who start as teens (about 17%, or one in six)[20] and among people who use marijuana daily (25–50%).[21,22]

143. SECURITY FOR MARIJUANA FARMS AND DISPENSARIES

For those who either cultivate or sell marijuana, it is important that they know how to protect their investment—equipment, inventory, products—and above all, their employees. The marijuana industry certainly comes with its own security challenges.

The legalization of recreational marijuana in Colorado and Washington introduced a new element for the cannabis industry in the United States—effective security that "fits" with this industry. Medicinal marijuana is legal in 23 states, but it is still considered a Schedule 1 controlled substance by the US government, which makes growing and selling marijuana illegal under federal law. This elevates the security situation for marijuana farms and dispensaries to a new level because many banks are reluctant to accept money that is generated from the sale of marijuana, so this has forced the industry to be an all-cash business.[23] This has led to the development of "specialty" security companies for a niche market. These "specialty" security companies not only protect product and cash on hand but also are responsible for securing the perimeter of the property, access control

[17] https://www.drugabuse.gov/publications/drugfacts/marijuana.
[18] Anthony, 1994.
[19] Lopez-Quintero 2011.
[20] Anthony, 2006.
[21] Hall W, Pacula RL. *Cannabis use and dependence*. UK: Cambridge University Press; 2003.
[22] https://www.drugabuse.gov/publications/drugfacts/marijuana.
[23] http://www.securityinfowatch.com/article/11601437/booming-cannabis-industry-presents-wealth-of-opportunities-to-security-system-installers-manufacturers.

in and out of areas and buildings, monitoring video surveillance and response, monitoring the intrusion detection systems, and providing ongoing consulting services; they have to constantly monitor the temperature and lighting within the growing facilities. It is important that marijuana farms and dispensaries consider all possible threats, have state-of-the-art technology as a part of their security master plans, and ensure that the security operation is efficient and either minimizes or eliminates any security vulnerability.

CNN reports that there are now big-box stores, named "weGrow," that offer marijuana-growing equipment, supplies, and services (including recommendations for security) and they are being called, the "Walmart of Weed."[24] None of the "weGrow" stores actually sell marijuana, but they advertise that their services and products are designed especially for cultivating marijuana. This is a perfect example of the premise, supply, and demand.

"weGrow" also offers a "Dispensary Security Plan" that covers facility as well as operational security that is touted as something that "…every dispensary or cultivation owner must have! Essential document for anyone that plans to own a marijuana dispensary." It includes a sample security plan and advertises that custom plans are also available. The security plans are designed to "minimize security exposure and prevent breaches before they even occur. However, in the event that preventative measures fail, the Operational Security Plan is designed to quickly observe, monitor, protect, counter and report any situations that do occur."[25]

The Facility Security Plan includes:

- Location and site security
- Secured employee parking
- Around the clock coverage
- Security surveillance systems (closed-circuit television)
- Maintenance of security systems
- Access control/ingress and egress
- Perimeter security
- Product security
- Fire alarm system
- Intrusion alarm system

The Operational Security Plan includes:

- Security threats
- Transactional security
- Delivery security
- Hazardous weather
- Human resource policies

[24] http://www.cnn.com/2011/US/05/31/arizona.marijuana.superstore/index.html?iref=allsearch.

[25] http://wegrowstore.com/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=35&vmcchk=1&option=com_virtuemart&Itemid=262.

- Employee security training
- Inventory control
- Guest, media, and visitor procedures
- Neighborhood involvement
- Emergency response
- Contingency planning[26]

The "specialty" security companies are meeting the needs of the marijuana industry because some dispensary owners have stated that ADT, the largest security provider in the nation has dropped or is refusing to accept customers in the marijuana industry. ADT told CNN Money it will not "sell security services to businesses engaged in the marijuana industry because it is still illegal under federal law."[27]

Owners in the marijuana cultivation and dispensary business state that they are concerned not only with thieves but also with federal authorities who are eager to see them put out of business.[28]

With demand for security services to protect the marijuana industry, there is certainly not a shortage of opportunities for security professionals.

144. THE INTERNET OF THINGS

The significant technology expansion that is about to happen: IoT, Sensors and Analytics the Internet of Things has truly changed the technology landscape. In fact, many of the things we only dreamt about a few short years ago are now commonplace. As IoT begins to converge with sensors and analytics it is evident that the technology landscape is poised to change yet again. Moreover, that change will affect industries across the board. It is not hard to imagine some of those scenarios that are probably just around the corner. In a not too distant future, an interesting set of events will be taking place in a single day.

VIRTUAL VISIT

A family checks in to medical reception for one member's outpatient procedure. The patient is given an RF ID tag and a family member's smartphone NFC function is activated via the hospital's patient care application. Both are beacons, meaning they present a specific set of information securely to nearby sensors. The patient is already in preoperative stage, and the family member with the smartphone walks over to a self-serve kiosk that senses they are nearby. A greeting is given, a simple yet trusted identity verification is performed, and the kiosk pulls up a video of their loved one resting comfortably awaiting surgery. "We'll be back before you know it," the nurse says

[26] http://wegrowstore.com/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=35&vmcchk=1&option=com_virtuemart&Itemid=262.
[27] http://money.cnn.com/2013/04/29/smallbusiness/marijuana-security/.
[28] http://money.cnn.com/2013/04/29/smallbusiness/marijuana-security/.

reassuringly to the intelligent video surveillance dome camera, knowing the patient's family is anxiously waiting. Within the hour, a notification pops into the family's smartphone, letting them know the patient is in recovery. A return to the kiosk lets them say a quick "hello." Virtually no buttons have been pushed or complex device registration performed; the video surveillance camera, application and connectivity did (almost) all the work. With the outpatient census at this particular smart health care center being quite high, this same cycle is repeated over and over again, simultaneously and with improving optimization of the services. A facial recognition application verifies the patient location on check-in when a follow-up visit is required. For today's challenging and increasing patient "elopements" or unplanned wandering off-premises of longer term care individuals, the facial recognition App and mobile notification to a security officer's smartphone becomes another tool in potentially saving a life. The data relating to the quality and frequency of this interaction are logged so that the smart application can reserve more Healthcare Center infrastructure services during peak periods. (The significant technology expansion that's about to happen: IoT, Sensors and Analytics,[29] permission obtained to reproduce.)

145. DRONES (UNMANNED AERIAL VEHICLES)

Drones or unmanned aerial systems have most often been associated with the military, but they are also used for search and rescue, surveillance by law enforcement, traffic monitoring, weather monitoring, firefighting, monitoring crops and livestock, and inspecting critical infrastructure such as pipelines and utility lines.[30] The aircraft can be remotely controlled or be guided though software-controlled flight plans working with a Global Positioning System.

The increased popularity of drones for both recreational and commercial use has prompted the FAA to release new guidelines for drone operations. Drones used for recreational or hobby purposes have become an increasing safety issue for pilots and aircraft.

146. CRIME PREVENTION THROUGH INTEGRATED PROBLEM SOLVING: BROKEN WINDOWS

Have you ever conducted a risk assessment only to find that the property was the worst of the worst? The housing unit was gang infested with open selling of drugs on the sidewalk. Even the homeless were working for the drug dealers, and they were given cell phones to call when they saw the police.

The facilities office was at the front of the complex, and the cameras that worked were at the rear up on the third floor unattended. There was a large complex of 240

[29] Steve Surfaro, 2016. http://www.securitymagazine.com/articles/87130-perimeter-defense-strategy-a-technology-guide-to-progressive-and-cost-saving-target-hardening. Permission was obtained from Mr. Sufaro.

[30] whatis.techtarget.com/definition/drone.

units with two small dumpsters and trash everywhere on the grounds. Windows were boarded up; I originally thought they had several fires, but it was to prevent them from being broken into. Law enforcement refused to respond without necessary backup. Truly a horror show.

George Kelling one of the authors of *Broken Windows* (1982) along with James Q. Wilson has said "*we must reduce disorder and you will reduce crime*." The Former Commissioner of the New York Police William Bratton has said "*The strategy is sending a strong message to those who committed minor crimes that they will be held responsible for their acts.*"

The QR-R Code shown deals with a set of articles titled "Using Crime Prevention Through Environmental Design in Problem Solving" by Diane Zahm.

SUGGESTED STRATEGIES

- Community partnerships formulated
- Communication with law enforcement improved
- Police coverage with K-9
- Law enforcement as resident of complex
- A police substation established
- Tenants who are dealing become evicted
- Lighting increased
- Security surveillance system fixed
- Security officers assigned
- Neighborhood watch established
- Take back control of public and private space
- CPTED security landscape implemented
- Chronic issues addressed and not ignored

147. MONTREAUX DOCUMENT[31]

The full title is "*The Montreux Document - on pertinent international legal obligations and good practices for States related to operations of private military and security companies during armed conflict*."

The Montreaux Document was published on September 17, 2008, and is the first international document to describe international law as it applies to the activities of

[31] https://www.icrc.org/eng/resources/documents/publication/p0996.htm.

private military and security companies, whenever these are present in the context of an armed conflict.

Its purpose is to ensure that the actions of private security providers do not contravene human rights or international humanitarian law, specifically, torture or cruel, inhuman, or degrading treatment; prohibition and awareness of sexual exploitation and abuse; as well as recognition and prevention of human trafficking and slavery.

Source: Craig McQuate.

148. EMERGING TRENDS IN PHYSICAL SECURITY

INTRODUCTION

There is no doubt that technology will advance our profession. Almost monthly you can read of advancements. China, for example, is trying to be proactive and address precrime with the help of China Electronic Technology Group who seek to develop software to collate data on jobs, hobbies, consumption habits, and other behavior for the purpose of predicting terrorist acts before they strike.

- In California, a group of individuals are attempting to prevent crime based on software and crime analysis, which records crime data that advise on police presence in specific locations to reduce crime.
- Research into software will continue, and RFID technology and smart home devices will also play a bigger role in the future. Applications for new technology will expand over time and how we find new ways to use it.
- Metal detectors will become bigger than ever, especially the Garrett model PD-6500i unit.
- We are currently seeing the birth of cyber investigation, cyber forensics, and cyber certifications. Also, more women will be in this field going forward.
- Optical turnstiles combined with biometrics is going to be big.
- Body cameras for private security is in the future.
- Stand-alone access control readers to be used in compliance with standards.
- Conclusion: *Times have changed, and we also must change or be behind the curve.*

Emerging Trends in the past 5 years:

1. IT infrastructure protection planning
2. IT infrastructure as a single strategic plan
3. Mitigation strategies
4. IP video and digital video
5. IP security provisions
6. Security IP edge device
7. HD cameras and monitors
8. Video analytics
9. Visible light cameras

10. Thermal imaging and cameras
11. Thermal imaging sensors
12. Perimeter protection
13. Layers of protection analysis and IoT
14. Visitor management systems
15. Mass notification
16. Active shooter/active assailants
17. Cloud storage and computing for security
18. Advancement of CPTED
19. Contractor prequalification
20. Emergency management and planning for disasters
21. Software for physical security maintenances
22. Laser communication
23. Drones becoming a safety issue
24. Encryption
25. Critical thinking
26. Soft targets vs. target hardening and emergency management
27. Establishment of countermeasures and deterrents
28. Embracing the beast
29. Social media monitoring software
30. ASIS and NFPA Active Shooter/Active Assailant Initiative

149. TARGET HARDENING

The emphasis on design and use deviates from the traditional target hardening approach to crime prevention. Traditional target hardening focuses predominantly on denying access to a crime target through physical or artificial barrier techniques (such as locks, alarms, fences, and gates). Target hardening often leads to constraints on use, access, and enjoyment of the hardened environment. Moreover, the traditional approach tends to overlook opportunities for natural access control and surveillance. The term *natural* refers to deriving access control and surveillance results as a by-product of the normal and routine use of the environment. It is possible to adapt normal and natural uses of the environment to accomplish the effects of artificial or mechanical hardening and surveillance. Nevertheless, CPTED employs pure target hardening strategies, either to test their effectiveness when compared with natural strategies or when they appear to be justified as not unduly impairing the effective use of the environment.

As an example, a design strategy of improved street lighting must be planned, made efficient, and evaluated in terms of the behavior it promotes or deters and the use impact of the lighted (and related) areas in terms of all users of the area (offenders, victims, other permanent or casual users). Any strategy related to the lighting strategy (e.g., block-watch or neighborhood watch, 911 emergency service, police patrol) must be evaluated in the same regard. This reflects the comprehensiveness of

the CPTED design approach in focusing on both the proper design and effective use of the physical environment. Additionally, the concept of proper design and effective use emphasizes the designed relationship among strategies to ensure that the desired results are achieved. It has been observed that improved street lighting alone (a design strategy) is ineffective against crime without the conscious and active support of citizens (in reporting what they see) and police (in responding and conducting surveillance). CPTED makes an effort to integrate design with physical security, citizen and community action, and law enforcement strategies to accomplish surveillance consistent with the design and use of the environment.

CPTED adds a new dimension by incorporating the following elements into space design and management:

- Natural access control. Your space should give some natural indication of where people are allowed and not allowed. Do not depend just on locks, alarms, surveillance systems, and security officers, but make security part of the layout (see landscape security).
- Natural surveillance. Again, traditional factors like good lighting are important, but do not overlook a natural factor such as a strategically placed window or the placement of an employee work station.
- Territorial reinforcement. This is an umbrella concept, embodying all natural surveillance and access control principles. It emphasizes the enhancement of ownership and proprietary behaviors.

The CPTED proposes that the proper design and effective use of the built environment can lead to a reduction in the opportunity, fear, and incidence of predatory stranger-to-stranger-type crime, as well as result in an improvement of the quality of life[32]. Crime prevention design solutions should be integrated into the design and function of the buildings, or at least the location where they are being implemented.

In his writings on CPTED, Tim Crowe stated, “It is clear that light affects human behavior and too much or too little light will have different effects. It is now generally accepted that performance improves and fatigue levels drop in direct proportion to increased levels of light, but it also relates to the work or play environment.”

Source: Crowe T, Fennelly LJ, CPTED. 3rd ed.: Elsevier; 2013.

150. PROACTIVITY

Proactivity is the anticipation of types of problems or incidents, for example, potential for unauthorized access to a building and potential for people or property to be endangered by such a breach. It also involves planning ways to deal with them and implementing preventive countermeasures, for example, the initiating badge entry

[32] National Crime Prevention Institute, University of Louisville, Marianna Perry, CPP 2008.

and access control and appointing a well-trained staff member to work toward the reduction of crime and criminal activity.

Proactivity is also predicting specific possibilities to avert incidences or to deal with them appropriately when they occur. It is the difference between the general and the particular required planning that encompasses a wide range of possibilities compared with predicting specific possibilities.

Dean Wilson, Professor of Criminology, School of Law, Politics and Sociology, University of Sussex, UK, stated in his paper on precrime "Pre-crime aims to pre-empt 'would-be criminals' and predict future crime. Although the term is borrowed from science fiction, the drive to predict and pre-empt crime is a present-day reality" (2016 Wilson).

In particular, these terms like, *avoid, predict, and common sense*; predicting implies foreknowledge: what your common sense tells you can be hard to explain to one with no common sense. It is more than a mere suspicion or knowledge that an incident is about to occur. You have to be very proactive in your thinking, beyond common sense. You must consider being proactive and develop a set of performance goals by defining common working practices, and each person has to be accountable for them.

CONCLUSION

On completion of this book, we realized that we may have missed an item here or there but we did our best. We put in material we felt is current and needed as we all go forward. OSHA material was included because its being used in assessments, and fire information was updated; actually the whole book has been updated. Deterrents were spelled out, but the overall concept of the book is intact. We hope you enjoyed this text.

Index

'*Note:* Page numbers followed by "f" indicate figures, "t" indicate tables and "b" indicate boxes.'

A

Access cards, 12–13
  capacitance cards, 13
  magnetic cards, 12
  optical cards, 13
  proximity cards, 12
  smart cards, 13
  weigand cards, 12
Access control, 20, 71
  biometric, 13
  and surveillance, 112–113
Access control for security/protection officer, 11–13
  card readers, 13
  EAC, 11–12
Active assailant response, 96
Active security, 73
Active shooter response (ASR), 96
ADA. *See* Americans with Disabilities Act (ADA)
AHJ. *See* Authority Having Jurisdiction (AHJ)
Alarm system. *See* Intrusion detection system
American National Standards Institute (ANSI), 5
American Society for Industrial Security (ASIS), 1, 82, 159
  Standards and Guidelines, 5–6
Americans with Disabilities Act (ADA), 128
  compliance and security operations, 152
Ammonium phosphate, 116
ANSI. *See* American National Standards Institute (ANSI)
ANSI/ASIS Chief Security Officer, 6b
Anticipation of crime rate checklist, 97–98
Architects, designing security with, 89–91
Architectural design guidelines, 90
Area lighting, 46
Art of training, 61–64
  controlling class, 62–63
  golden rule, 64
  handouts, 63
  lecturing *vs*. teaching, 62
  nervousness, 63–64
  planning, 63
  recording devices, 64
  Visual Aids, 61–62
  voice control, 63
ASIS. *See* American Society for Industrial Security (ASIS)
ASR. *See* Active shooter response (ASR)
Asset protection, 8
  plan, 88
Audio recording, legal issues with, 163
Authority Having Jurisdiction (AHJ), 125
Automatic sprinklers, 125
Awareness, 27

B

Badges, 10–11
Bar codes, 11
Barrier(s)
  perimeter, 4, 82
  physical, 3–4
  planning, 4–5
  protective, 7
  symbolic, 23–24
Biometric access control, 13
Biometric devices, 13
Body cameras for law enforcement and private sector, 162–163
  department, 163
  legal issues with audio recording, 163
  training, 163
Broken Windows, 110–111
Budgeting, 67–68
Budgets: leasing versus purchase, 66–67
Building access: windows and glass, 40–43
Building design
  exterior access checklist, 30–31
  interior checklist, 29–30
Building interiors, 28–29
Building site security and contractors, 75–76
Buildings, commercial, 48
Bureau of Justice Statistics, 100
Burglary-resistant glass, 7
Business Continuity Planning, 137–138
Business Dictionary, 95

C

Cabinets, 72
Cannabinoid drug effects, 164
Cannabis sativa, 163
CAP Index, 97
Capacitance cards, 13
Carbon dioxide (CO_2), 116, 119
  flooding systems, 127

Card access systems, 10, 12–13
  capacitance cards, 13
  magnetic cards, 12
  optical cards, 13
  proximity cards, 12
  smart cards, 13
  weigand cards, 12
Card readers, 11–13
Cardiopulmonary resuscitation (CPR), 146
CCTV. *See* Closed-circuit television (CCTV)
Central stations, 50
CF. *See* Commercial Facilities (CF)
CFSSA. *See* Commercial Facilities Sector-Specific Plan (CFSSA)
Chain link fence, 7, 104
  perimeter lighting and, 46
Checklists
  for anticipation of crime rate, 97–98
  for designing for security, 18
  for emergency exit doors, 156–157
  for exterior building design, 30–31
  for fire prevention and suppression, 103–105
  for ingress and egress controls, 143–144
  for interior building design, 29–30
  for intrusion detection system, 50–51
  for security/protection officer inspection, 57–59
  for security/protection officers, 56–57
  for smoke alarm systems, 122–123
Chemical fire suppression systems, 127
Chemical storage, 71–72
"Closed" parking garage, 111
Closed-circuit television (CCTV), 4, 14, 52–53, 138
  and lighting, 23f
  for security/protection officer, 11
CO_2. *See* Carbon dioxide (CO_2)
Combination lock, 70
Commercial buildings, 48
Commercial Facilities (CF), 131
Commercial Facilities Sector-Specific Plan (CFSSA), 131
Communication, 57, 144
Components
  basic EAC system, 12
  of intrusion detection system, 50
  security, 38
Comprehensive plans, 90
Computer-savvy hackers, 159
Computers, fire protection, 126–127
Concertina wire, 7–8
Construction suitable for occupancy, 125
Contractors and building site security, 75–76
Control panel, 50, 121
Control signs, 32
Countermeasures, assessment of, 87
CPR. *See* Cardiopulmonary resuscitation (CPR)
CPTED. *See* Crime Prevention Through Environmental Design (CPTED)
Crime
  fear of, 27
  intelligence analysis, 101
  necessary for, 97
  problems, 101
  trends, 101
  in United States, 99
Crime analysis, 100–101
  crime intelligence analysis, 101
  problems, 101
  trends, 101
Crime and crime prevention techniques
  anticipation of crime rate checklist, 97–98
  CPTED strategies, 108–109, 112–113
  crime analysis, 100–101
  crime reporting, 98–100
  deterrents, 103–105
  environmental security, 109–113
  "If You See Something, Say Something" campaign, 103
  parking lots and parking garages, 111–112
  residential security, 105–107
  situational, 101–103
  space, 107–109
  through integrated problem solving, 110–111
  triangle, 97
Crime prevention, 19
  design and use, 3–4
  four D's, 79
  through integrated problem solving, 170–171
  situational, 101–103
  strategies, 9
  triangle, 97
Crime Prevention Through Environmental Design (CPTED), 3–4, 19, 19f
  assessment, 24–25
  design review, 89–91
  issues/recommendations, 25–26
  maintenance, 22–24
  measuring and evaluating, 26–27
  planning, 89–91
  principles, 103
  program, 9
  security applications and, 31–32
  strategies, 19–24, 108–109, 112–113
Crime rate checklist, anticipation of, 97–98
Crime reporting, 98–100
  crime in United States, 99
  NCVS, 100
  NIBRS, 99–100

Critical infrastructure networks, 162
Cyber
  activity, 161
  attack, 162
  crime, 162
  criminals, 162
  threat actors, 161–162
  threats, 160–161

D

Data center and server security, 68–70
Data collection, 80
Day-to-day operations of protection officer, 57
Defense-in-depth. *See* Onion-skin concept
Defensible space, 104, 110
Department of Labor (DOL), 145
Design of building
  exterior access checklist, 30–31
  interior checklist, 29–30
Designing security and working with architects
  CPTED planning and design review, 89–91
  LEED, 89
  review process, 91
Designing security with architects, 89–91
Detection devices, 51
Deterrents, 103–105
Digital voice alarms, 38
Directional signs, 31
DMAs. *See* Door management alarms (DMAs)
DOL. *See* Department of Labor (DOL)
Door management alarms (DMAs), 39
Door(s)
  digital voice alarms, 38
  DMAs, 39
  exit alarms, 39
  exposed hinges, 35
  exterior doors, 38
  frames, 35–38
  management, 38–39
  model door numbering system, 39–40
  physical entry and access control doors, 32
  prop alarms, 39
  sample applications, 38–39
  strike plates, 36–37
  viewers, 37–38
Dronabinol, 165
Drones, 170
Dry chemical extinguishers, 116
Dynamic alarm management, 88–89
Dynamic risk, 105

E

EAC systems. *See* Electronic access control systems (EAC systems)
Earthquakes, 140
ECC. *See* Emergency Command Center, (ECC)
Effective physical security, 47
Egress and ingress controls checklist, 143–144
Electronic access control systems (EAC systems), 11–12
  access cards, 12
  biometric access control, 13
  card readers, 13
  security/protection officer and technology tools, 16
Elevator, 153–154
  safety, 154
Emergency (blue light) phones/call stations, 74
Emergency Command Center, (ECC), 128
Emergency organization, effective, 126
Emergency planning, 127–129, 139–140
  active shooter incidents, 133–134
  ADA compliance and security operations, 152
  assessing risks, 131
  best practices, 141–143
  determining vulnerability, 141
  elevator and escalator safety issues, 153–154
  emergency exit doors, 156
  emergency policies and procedures training, 152–153
  emergency procedures and security operations, 146
  emergency response and life safety, 143
  emergency response plan, 141
  facility manager responsibilities, 132–133
  identifying assets, systems, and networks, 131
  implementing programs, 132
  ingress and egress controls checklist, 143–144
  managers, 129–134
  mass notification procedures, 144–145
  measuring progress, 132
  mutual aid associations, 138–139
  national response framework, 135–138
  occupational safety and health administration, 145
  OSHA emergency procedures and security operations, 150–152
  OSHA fact sheet, 146–150
  plan development and considerations, 139–141
  prioritizing, 132
  reinventing security performance, 145
  responsibilities, 134–135

Emergency planning (*Continued*)
set goals and objectives, 131
soft targets, 130–131
types of emergencies, 140–141
unsafe acts and unsafe conditions, 155–156
Emergency Support Function, 137
Emerging trends in physical security, 172–173
body cameras for law enforcement and private sector, 162–163
crime prevention through integrated problem solving, 170–171
cyber crime, 162
cyber threat actors, 161–162
cyber threats, 160–161
encryption, 160
internet of things, 169–170
marijuana, 163–167
Montreaux document, 171–172
proactivity, 174–175
security for marijuana farms and dispensaries, 167–169
social media, 159–160
target hardening, 173–174
Encryption, 160
Entrances, 22. *See also* Ingress and egress controls checklist
gates and, 3, 173
service entrance protection, 29
signs, 32
Entry-control stations, 111
Environment, 9–10
Environmental design, 9
Environmental security, 10, 104, 109–113
neighborhood and fear of crime, 109–110
Escalators, 154
safety, 154
Exclusion areas, 32
Exit alarms, 39
Expenses, unforeseen, 67
Exposed hinges, 35
Exterior building design checklist, 30–31
Exterior doors, 33, 38
Exterior number
position, 39–40
sizing, 40

F

Facility, ten qualities of a well-protected, 124–126
False alarms, 57, 123–124
fire alarms, 124
intrusion alarms, 95
smoke alarms, 121
FDA. *See* Food and Drug Administration (FDA)
Fear of crime, 27
Federal Bureau of Investigation, 99
Fences
barbed tape, 7
barbed wire, 7–8
chain link, 4–5, 7, 18, 46
concertina, 7–8
enhancements, 7–8
gates and, 3, 173
walls and, 3, 66
Files, safes, and vaults, 2
Fingerprints, 13, 70
Fire alarms, 124
Fire classes, 119–120
smoke detectors, 119–120
Fire inspections, 118–119
Fire prevention and suppression checklist, 120–121
Fire protection and safety, 115–116
classes of fire, 119–120
computers, 126–127
equipment maintenance, 123, 123t
fire extinguishers, 115
fire inspections, 118–119
FPPs, 117–118
high-quality fire extinguishers, 115–116
NFPA, 116–117, 116t–117t
qualities of well-protected facility, 124–126
reducing false alarms, 123–124
smoke alarms, 121–123
Fire protection programs (FPPs), 117–118
risk acceptance and transfer, 118
risk avoidance and risk reduction, 118
risk identification and risk assessment, 117
Floodlighting, 46
Floods, 140
Foam extinguishers, 116
Food and Drug Administration (FDA), 165
FPPs. *See* Fire protection programs (FPPs)

G

Garage doors, 34
Gatehouse lighting, 45
Gates
entrances and, 3, 173
fences and, 3, 173
Glass, building access, 40–43
Glass, burglary-resistant, 7
Grove, The, 113
Guard houses/guard booths, 65

H

Hacktivists, 162
Halon systems, 127
Hand geometry, 13, 70

"Hasp lock", 92
Hazards, special, 125
Heating, ventilation, and air conditioning (HVAC), 2
"Hierarchy rule", 100
Hinges, 33
Hollow core, 33
Housekeeping, good, 126
Human hackers, 159–160
Human Resources department, 2
HVAC. *See* Heating, ventilation, and air conditioning (HVAC)

I

Identification signs, 31
"If You See Something, Say Something" campaign, 103
IICD. *See* Infrastructure Information Collection Division (IICD)
Illumination, 44
  levels, 47–48
Improperly closed valve (lCV), 125
Inadequate security and security liability, 76–77
Independent protection layer (IPL), 82–83
Information Technology (IT), 125
Informational signs, 31
Infrared devices, 43
Infrastructure Information Collection Division (IICD), 131
Ingress and egress controls checklist, 143–144
Insiders, 161
Integrated problem solving, 110–111
Inspection of protection officer checklist, 57–59
Insurance, 85
Integration, security system, 87–88
Intelligent video. *See* Video analytics
Interior building design checklist, 29–30
Interiors, building, 28–29
Internal theft, 8–9
International Foundation for Protection Officers, 64–65
Internet-based social networking sites, 159
Intrusion detection system, 50
  checklist, 50–51
  components, 50
  device types, 51
Ionization, 120
Ionization-type alarms, 120
IPL. *See* Independent protection layer (IPL)
IT. *See* Information Technology (IT)

K

Key management, efficient, 49–50
Keys, 2, 13

L

Landscape ordinances, 90
Law enforcement, 99
Layered security. *See* Defense-in-depth
Layers of protection analysis (LOPA), 82–84, 83f
lCV. *See* Improperly closed valve (lCV)
Leadership in Energy and Environmental Design (LEED), 48–49, 89
Leasing versus purchase and budgets, 66–67
LED. *See* Light-emitting diode (LED)
LEED. *See* Leadership in Energy and Environmental Design (LEED)
Lethal weapons for security/protection officers, 56
Light-emitting diode (LED), 18
Lighting, 44
  area, 46
  brightness in parking garages, 74
  equipment and system design, 46
  floodlighting, 46
  perimeter, 46
  primary sources, 43–44
  protective, 44–45
  recommendations, 47–48
  security, 45–47
  systems, 45
Lines of defense. *See* Onion-skin concept
Loading docks, 70–71
Locking bar, 92
LOPA. *See* Layers of protection analysis (LOPA)

M

Magnetic cards, 12
Magnetometers, 16–17
Maintenance
  CPTED, 22–24
  fire protection equipment, 123
  physical security expenses and, 65–66
  smoke alarm systems, 122–123
Man-made disasters, 141
Management and staff, motivated, 124
Marijuana, 163–164
  long-term effects of marijuana, 166–167
  marijuana addiction, 167
  for medicinal purposes, 164–167
  security for marijuana farms and dispensaries, 167–169
  short-term effects of marijuana, 166

Mass Notification Program, 144
Master plan, 92, 95–96
Metal, 33
Metal detectors, 16–17
Microwave devices, 51
Mirrors, 66
Monitored intrusion detection systems, 107
Montreaux document, 171–172

N

National Crime Victimization Survey (NCVS), 99–100
National Fire Protection Association (NFPA), 116–117, 116t–117t
  NFPA 1600 tool, 128, 142
National Incident-Based Reporting System (NIBRS), 99–100
National Institute of Building Sciences, 113
National response framework, 135–138
  elements of emergency contingency plan, 136–138
  FEMA, 136
  hazards, 136
  vulnerability and risk assessment, 135
Natural access control, 113
Natural disasters, 140
Natural surveillance, 110, 112
Natural surveillance through electronics, 22
NCVS. *See* National Crime Victimization Survey (NCVS)
NFPA. *See* National Fire Protection Association (NFPA)
NIBRS. *See* National Incident-Based Reporting System (NIBRS)
Nonlethal weapons for security/protection officers, 56
Nonreactive stains, 74

O

Occupational Safety and Health Administration (OSHA), 128, 145
  design and construction requirements, 147–148
  emergency exit routes, 146
  emergency procedures and security operations, 150–152
  enforcement, 145
  fire safety in workplace, 148–150
  regulations, 146
  requirements for exits, 147
  safety features for exit routes, 147
  workplace exit routes, 147
Onion-skin concept, 82–83
Onion-skin concept, 82
"Open" parking garage, 111
Optical cards, 13
Optical turnstiles, 14–15
  solutions, 15–16
OSHA. *See* Occupational Safety and Health Administration (OSHA)

P

Padlock, 91–92
Palm prints, 13
Parking lots and garages, 111–112
  CPTED strategies, 112–113
  Los Angeles example, 113
Passive security, 73
Patrol tours, 45
Perimeter, 4
  barrier, 4
  lighting, 46
Personal protective equipment (PPE), 151
Personnel gate ingress and egress controls checklist, 143–144
Pet doors, 34
Photoelectric detectors, 120
Photoelectric smoke detectors, 120
Physical asset protection, 5
Physical barriers, 3–4
Physical entry and access control doors, 32
Physical security, 1, 7
  effective, 1–2
  expenses and maintenance, 65–66
  policies and procedures, 6–7
Physical Security Information Management (PSIM), 88–89
Physical systems, 95–96
Planning
  barriers, 4–5
  CPTED planning and design, 89–91
  emergency, 127–129, 139–143
  "Master Plan", 95–96
  to workplace emergencies, 150–152
Positive locking methods, 92
Possible maximum loss, 105
Power sources, 118
PPD. *See* Presidential Policy Directive (PPD)
PPE. *See* Personal protective equipment (PPE)
Premises security liability, 76
Presidential Policy Directive (PPD), 135
Pressurized water models, 116
Primary lighting sources, 43–44
Private space, 108
Proactivity, 174–175
Probable maximum loss, 105
Professional certifications, 64–65
Property crime, 99

Property management. *See also* Crime Prevention Through Environmental Design (CPTED); Door(s); Security/protection officers(s)
access control for security/protection officer, 11–13
art of training, 61–64
ASIS International Standards and Guidelines, 5–6
asset protection, 8
badges, 10–11
bar codes, 11
barrier planning, 4–5
budgeting, 67–68
budgets, 66–67
building access, 40–43
building site security and contractors, 75–76
card access systems, 10
chemical storage, 71–72
crime prevention, 19
critical areas in storage facility, 72
data center and server security, 68–70
designing for security, 18
designing security and site layout, 17
EAC system, 16
efficient key management, 49–50
emergency (blue light) phones/call stations, 74
environment, 9–10
exterior building design, 30–31
fence enhancements, 7–8
guard houses/guard booths, 65
illumination, 44
inadequate security and security liability, 76–77
interior building design, 28–30
internal theft, 8–9
intrusion detection system, 50–51
LEED, 48–49
lighting recommendations, 47–48
loading docks, 70–71
magnetometers, 16–17
monitoring images, 53–54
optical turnstile solutions, 15–16
parking facility security, 72–74
physical barriers, 3–4
physical security, 1–2, 7
physical security expenses and maintenance, 65–66
physical security policies and procedures, 6–7
primary lighting sources, 43–44
professional certifications, 64–65
protective lighting, 44–45
security lighting, 45–47
security surveillance system, 51–52
signage, 31–32
site and target hardening, 2–3
tailgating, 13–15
thermal imaging cameras, 54
turnstiles, 13–15
vandalism, 27–28
video analytics, 54
video surveillance systems, 52–53
Protection officer and technology tools, 16
Protective lighting, 44–45
Proximity cards, 12
PSIM. *See* Physical Security Information Management (PSIM)
Public space, 107
Purchase versus leasing and budgets, 66–67
Pure risk, 80, 105
Push button lock, 74

Q

QR-R Code, 171
Qualitative methods, 81
Quantitative methods, 81

R

Reactive stains, 74
Residential security, 105–107
home safety and security, 106–107
Retina patterns, 13
Revolving doors, 32–33
Risk acceptance, 85
and transfer, 118
Risk analysis, 81
Risk and vulnerabilities assessment
active assailant response, 96
ASR, 96
assessment of countermeasures, 87
asset protection plan, 88
defense-in-depth, 82
designing security and working with architects, 89–91
deter, detect, delay, and deny, 79
five techniques to deal with identified risks, 84–87
LOPA, 82–84, 83f
master plan, 92
padlocks, 91–92
physical systems, 95–96
PSIM, 88–89
qualitative *vs*. quantitative methods, 81
risk analysis, 81
security master plans, 93
security plan design, 5 and 10-year, 93–95
security system integration, 87–88
soft target, 79
threat risk assessments, 80

Risk assessment, 97–98, 117
  analysis, 81
  program, 6
Risk avoidance, 84, 118
Risk identification, 117
Risk loss reduction, 85
Risk management, 105
Risk mitigation strategies, 85–87
Risk reduction, 86, 118
Risk retention, 86
Risk sharing, 87
Risk spreading, 85
Risk transfer, 86
Risk transference, 85
Risks, techniques with, 84–87

S

Safes, 2, 82
Sample applications, 38–39
SAS. *See* Statement on Auditing Standards (SAS)
Secure areas, 70
Security
  assessment, 108
  and contractors for building site, 75–76
  countermeasures, 105
  designing and layout of site for, 17
  designing for, checklist for, 18
  designing with architects for, 17
  environmental, 109–113
  lighting for, 45–47
  management standard, 5
  master plan, 92–93
  parking facility, 72–74
  residential, 105–107
  surveillance applications and CCTV for, 138
  surveillance system, 51–52
  survey for, 97–98
  system integration, 87–88
Security Cultural Community, 159
Security lighting
  area lighting, 46
  controls, 46
  floodlighting, 46
  goals, 47
  lighting equipment and system design, 46
  lighting requirements, 45
  lighting systems, 45
  perimeter lighting, 46
  wiring, 46
Security plan design, 5 and 10-year, 93–95
Security/protection officers(s)
  checklist, 56–57
  day-to-day operations, 57
  inspection checklist, 57–59
  lethal and nonlethal weapons for, 56
  operations, 55–56
  and professionalism, 64
  training for, 59–61
Semiprivate space, 107
Semipublic space, 107
“Shackle-less” padlock, 92
ShatterGARD, 43
Signage, 31–32
  control signs, 32
  other signs, 32
  security applications and CPTED, 31–32
  warning signs, 32
Site hardening, 2–3
Site layout and designing security, 17
Situational crime prevention, 101–103
Sliding glass doors, 34
Smart cards, 13
Smoke alarms, 121
  choosing, 121
  installation, 121
  position, 121
  systems, 122–123
  trend, 121
Smoke detectors, 119–120, 124
  ionization, 120
  photoelectric, 120
Snowstorm, 140
Social engineers. *See* Social hackers
Social hackers, 159–160
Social media, 159–160
  risks, 160
  vulnerability of social networking sites, 160
Sodium bicarbonate, 116
Soft target, 79
Solid wood/solid wood core, 33
Space, 107–109
SPC. 2 Standard, 6b
Special hazards, 125
Spreading, 37
Sprinklers, automatic, 125
SSAE. *See* Statement on Standards for Attestation Engagements (SSAE)
Statement on Auditing Standards (SAS), 68
Statement on Standards for Attestation Engagements (SSAE), 68
Storage facility, critical areas in, 72
Storm door, 34
Strengths, weaknesses, opportunities, threats (SWOT), 103
Strike plates, 36–37
Subdivision regulation, 90

Supply chain risk management, 6
Surface parking lot. *See* "Open" parking garage
Surveillance, 113
  CCTV and security applications for, 138
  natural, 22
SWOT. *See* Strengths, weaknesses, opportunities, threats (SWOT)

T

Tailgating and turnstiles, 13–15
Target hardening, 2–3, 173–174
Territorial reinforcement, 112
Territoriality, 110
Terrorists, 161
Tetra hydrocannabinol (THC), 163
Thermal imaging cameras, 54
Threat potential, lists useful for, 10
Threat risk assessment, 79–80
Three-D concept, 4
Thunderstorms, 140
Topping-up lighting, 45
Trespassers, dealing with, 107
Tsunami, 140
Turnstile solutions, optical, 15–16
Turnstiles, 13–15
Turnstiles and tailgating, 13–15

U

Uniform Crime Reporting (UCR), 81, 98
Unmanned aerial systems, 170
US. Green Building Council (USGBC), 89

V

Vandalism, 27–28
Vaults, 2, 51, 82, 97–98
Vehicular doors, 33
Video analytics, 54
Video badging, 10
Video surveillance, 52, 72
  systems, 52–53
Violent crime, 99
Virtual visit, 169–170
Voice alarm, digital, 38
Vulnerability
  assessment, 80, 88
  of social networking sites, 160

W

Walls and fences, 3–5
"Walmart of Weed", 168
Warning signs, 31–32
Water supply adequate for occupancy, 125
Weigand cards, 12
Well-protected facility, ten qualities of, 124–126
Williams–Steiger Occupational Safety and Health Act of (1970), 145
Windows, 40–43
  awning-type wood and metal type of, 42
  commercial buildings and, 45
  double hung wood type of, 41
  factors for selection of type and size of, 40
  glass/glazing, 42–43
  protection types available for, 7
  purpose of, 40
  securing windows with locks, 43
  steel security screens, grilles, or bars, 42
  types of, 41–42
  weakest part of, 7

Z

Zoning ordinances, 90